

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2004年6月3日 (03.06.2004)

PCT

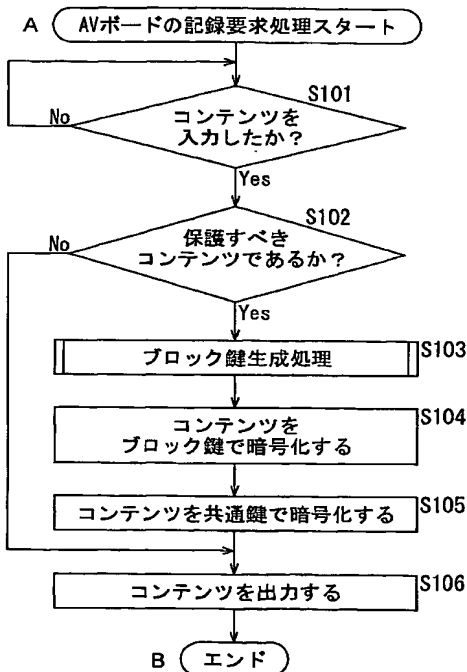
(10) 国際公開番号  
WO 2004/046936 A1

- (51) 国際特許分類: G06F 12/14, G09C 1/00, G11B 20/10 (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (21) 国際出願番号: PCT/JP2003/013752
- (22) 国際出願日: 2003年10月28日 (28.10.2003) (72) 発明者; および
- (25) 国際出願の言語: 日本語 (75) 発明者/出願人 (米国についてのみ): 千秋進 (SEN-SHU, Susumu) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願 2002-336754 (74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒160-0023 東京都新宿区西新宿7丁目11番18号 711ビルディング4階 Tokyo (JP).
- 2002年11月20日 (20.11.2002) JP

[続葉有]

(54) Title: RECORDING SYSTEM AND METHOD, RECORDING DEVICE AND METHOD, INPUT DEVICE AND METHOD, REPRODUCTION SYSTEM AND METHOD, REPRODUCTION DEVICE AND METHOD, RECORDING MEDIUM, AND PROGRAM

(54) 発明の名称: 記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラム



A...START OF AV BOARD RECORDING  
REQUEST PROCESSING  
S101...CONTENT RECEIVED?  
S102...CONTENT TO BE PROTECTED?  
S103...BLOCK KEY GENERATION  
PROCESSING  
S104...ENCRYPT CONTENT WITH BLOCK KEY  
S105...ENCRYPT CONTENT WITH COMMON KEY  
S106...OUTPUT CONTENT  
B...END

(57) Abstract: A recording system and method, a recording device and method, an input device and method, a reproduction system and method, a reproduction device and method, a recording medium, and a program for protecting a content flexibly based on whether or not the content must be protected. When a mutual authentication unit (121) has already performed mutual authentication with an AV board (112) and a content received by the mutual authentication unit (121) has been encrypted with a common key, an input/output controller (122) judges that a content received via a bus (113) is to be protected on the bus (113) and, under control of a recording/reproduction processing unit (123), generates protection information "0", which indicates that the content should be protected on the bus (113), and records the generated protection information, as well as the content, on an optical disc (141). The present invention is applicable to an optical disc recording/reproduction device.

(57) 要約: 保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにした記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラムに関する。入出力制御部 122 は、相互認証部 121 により AV ボード 112 との間で相互認証がされ、かつ、相互認証部 121 に入力されたコンテンツが共通鍵で暗号化されている場合、バス 113 を介して入力されるコンテンツがバス 113 上で保護されるべきコンテンツであると判断し、記録再生処理部 123 を制御し、バス 113 上で保護すべきコンテンツであるという保護情報「0」を生成させ、生成された保護情報を、コンテンツとともに、光ディスク 141 に記録させる。本発明は、光ディスク記録再生装置に適用できる。



(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明細書

記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラム

## 5 技術分野

本発明は、記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラムに関し、特に、保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにした記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラムに関する。

## 背景技術

記録再生装置（例えば、CD-RW ドライブなど）においては、ディスクに記録または再生を行う場合、コンテンツを保護するために、正当な記録再生制御と不正コピーの防止が求められている。

例えば、特表 2002-521789 号公報には、ユーザデータとユーザコントロールデータにより構成されるデータフォーマットを用いて、ディスクに記録または再生を行うことが提案されている。

20 このようなデータフォーマットにおいては、そのユーザデータ部分に、ディスクに固有の ID であるディスク ID を作用させた鍵で暗号化して記録することによりコンテンツが不当なコピーから保護される。

また、特開 2002-84271 号公報には、図 1 に示される記録再生装置 1 が開示されている。

25 図 1 の例においては、記録再生装置 1 は、ドライブ 11、AV ボード 12 および専用バス 13 により構成される。ドライブ 11 は、記録再生処理部 21 を有し、AV ボード 12 は、AV コンテンツ処理部 31、コンテンツ保護部 32、入力部

3 3 および出力部 3 4 を有している。

記録再生処理部 2 1 は、光ディスク 4 1 が装着されると、光ディスク 4 1 に固有のディスク I D および R K B (Renewal Key Block) を取得し、専用バス 1 3 を介して、A V ボード 1 2 のコンテンツ保護部 3 2 に供給する。コンテンツ保護部 3 2 は、取得したディスク I D および R K B から得たディスク鍵を作用させた鍵を生成し、記憶する。

A V コンテンツ処理部 3 1 は、アンテナなどにより構成される入力部 3 3 を介して受信された著作権を保護する必要があるコンテンツを、コンテンツ保護部 3 2 に供給する。コンテンツ保護部 3 2 は、予め記憶されているディスク I D および R K B から得たディスク鍵などを作用させた鍵でコンテンツを暗号化し、保護すべきコンテンツとして、専用バス 1 3 を介して、記録再生処理部 2 1 に供給する。記録再生処理部 2 1 は、暗号化されたコンテンツを受信し、光ディスク 4 1 に記録する。

また、記録再生処理部 2 1 は、光ディスク 4 1 から所定の暗号化されたコンテンツを再生し、専用バス 1 3 を介して、コンテンツ保護部 3 2 に供給する。コンテンツ保護部 3 2 は、暗号化されたコンテンツを、ディスク I D および R K B から得たディスク鍵を作用させた鍵で復号し、A V コンテンツ処理部 3 1 に供給する。A V コンテンツ処理部 3 1 は、復号されたコンテンツを、例えば、MPEG (Moving Picture Experts Group) 方式でデコードし、再生する。出力部 3 4 は、再生されたコンテンツを出力する。

以上のように、ドライブ 1 1 と A V ボード 1 2 間においては、記録再生装置 1 内の専用バス 1 3 を介しているため、外部からアクセスされることはなく、ディスク I D または R K B を利用して、コンテンツを保護することができる。

図 1 の変形例として、図 2 に示されるような、記録再生装置 5 1 が考えられる。尚、図 2 において、図 1 における場合と対応する部分には対応する符号を付してあり、その説明は繰り返しになるので省略するが、図 2 の例の場合、ドライブ 1 1 と A V ボード 1 2 がバス 6 1 (汎用バス) を介して分離されている (例えば、

家庭内LAN(Local Area Network)などで分離されている)。

したがって、図2の例においては、バス61にディスクIDおよびRKBがそのまま流れてしまうため、これらが盗用される危険が生じる。例えば、コンテンツを記録する場合、HDD(Hard Disk Drive)71をバス61に接続することにより、バス61上にある「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」が吸い上げられ(モニターされ)、HDD71にコピーされてしまう。

図2の例の場合、HDD71には、以上のようにして吸い上げられた、16BのディスクID、数MBのRKB、および20GBの暗号化コンテンツ、並びに、数KBのプログラムが記憶されている。HDD71により、これらの「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」が、AVボード12に与えられると、AVボード12は、正当な光ディスク41から再生されたものとの識別ができないため、コンテンツを再生してしまう。

以上のように、吸い上げた「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」を、AVボード12に対して与える「なりすましドライブ」または「なりすましプログラム」は、再生実行型装置またはプログラムとして、一般的に流通されてしまう恐れがある。

したがって、ドライブ11とAVボード12が、バス61を介して分離している構成の記録再生装置51においては、正当なディスクでなくても、HDD71のように、何らかのメディアにコピーされ、流通されてしまう恐れがある。

そこで、図3に示されるような相互認証を行う記録再生装置81が提案される。図3の例においては、ドライブ11に相互認証部91が設けられ、AVボード12に相互認証部92が設けられ、それらの間で相互認証処理が実行されることにより共有された共通鍵を用いて暗号化することで、コンテンツの送受信が行われる。

これにより、記録再生装置 1 または記録再生装置 5 1 で記録された光ディスクと互換性があり、かつ、相互認証機能を有しない HDD 7 1 においては、「ディスク ID」、「RKB」および「ディスク ID および RKB から得たディスク鍵を用いて暗号化されたコンテンツ」がコピーされたとしても、その復号ができないので、実質的にコピーを不可能にすることができる。したがって、上述した「なりすましドライブ」または「なりすましプログラム」を防止することができる。

しかしながら、最近、暗号化コンテンツをフリーで提供するという超流通用途のため、あるいは、PC (Personal Computer) ストレージ用途のために、保護する必要がないコンテンツは、ユーザから見てコピー可能なように、バス 1 3 上では暗号化せずに記録、再生できるようにし、かつ、保護すべきコンテンツは、実質的にコピー防止できるようにすることが望まれている。

しかしながら、現在、一般の PC の HDD 7 1 には、相互認証処理を実行する機能が備えられていないため、記録再生装置 8 1 においては、HDD 7 1 には、保護すべき特定のコンテンツだけでなく、PC ストレージ用途のための保護不要のコンテンツまでもコピーすることができなくなってしまうといった課題があった。

## 発明の開示

20 本発明はこのような状況に鑑みてなされたものであり、保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにするものである。

本発明の記録システムは、入力装置は、入力されたコンテンツを保護するか否かを判断する判断手段を備え、記録装置は、判断手段により判断された結果に基づいて、コンテンツがバス上での伝送において保護すべきコンテンツであるか否かを示す保護情報を、コンテンツとともに記録媒体に記録する記録手段を備えることを特徴とする。

記録手段は、コンテンツの所定の単位ごとに保護情報を記録するようにするこ

とができる。

所定の単位は、2048バイトであるようにすることができる。

記録装置は、判断手段によりコンテンツを保護すると判断された場合、記録媒体のIDと記録媒体鍵を作用させてコンテンツを暗号化する暗号化手段をさらに  
5 備えるようにすることができる。

記録装置は、判断手段によりコンテンツを保護しないと判断された場合、少なくとも、記録媒体の記録媒体鍵を作用させてコンテンツを暗号化する暗号化手段をさらに備えるようにすることができる。

入力装置および記録装置は、それぞれ相互に認証する認証手段をさらに備える  
10 ようにすることができる。

入力装置は、判断手段によりコンテンツを保護すると判断された場合、バスへのコンテンツの送出前に、コンテンツを暗号化する第1の暗号化手段をさらに備え、記録装置は、判断手段によりコンテンツを保護すると判断された場合、記録手段によるコンテンツの記録前に、コンテンツを暗号化する第2の暗号化手段を  
15 さらに備えるようにすることができる。

判断手段によりコンテンツを保護しないと判断された場合、第1の暗号化手段は、バスへのコンテンツの送出前に、コンテンツを暗号化することを禁止するようにすることができる。

本発明の第1の記録方法は、入力装置は、入力されたコンテンツを保護するか  
20 否かを判断し、記録装置は、判断された結果に基づいて、コンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を、コンテンツとともに記録媒体に記録することを特徴とする。

本発明の記録装置は、バスを介して接続された他の装置と相互に認証を行う認証手段と、他の装置からバスを介して供給される第1の暗号化方法により暗号化  
25 されたコンテンツを復号する復号手段と、復号手段により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録手段とを備えることを特徴とする。

復号されたコンテンツを、第2の暗号化方法により暗号化する暗号化手段をさらに備えるようにすることができる。

暗号化手段は、記録媒体のIDと記録媒体鍵を作用させて復号されたコンテンツを暗号化するようにすることができる。

- 5      記録手段は、他の装置からバスを介して供給されたコンテンツが、第1の暗号方法により暗号化されていないコンテンツの場合、コンテンツを、バス上での伝送において保護すべきコンテンツでないことを示す保護情報とともに記録するようにすることができる。

- 10      本発明の第2の記録方法は、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

- 15      本発明の第1の記録媒体のプログラムは、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

- 20      本発明の第1のプログラムは、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

- 25      本発明の入力装置は、バスを介して接続された記録装置と相互に認証を行う認証手段と、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを第1の暗号化方法で暗号化する第1の暗



号化手段と、第 1 の暗号化手段により暗号化されたコンテンツを、バスを介して記録装置に供給する供給手段とを備えることを特徴とする。

第 1 の暗号化手段により暗号化されたコンテンツを、第 2 の暗号化方法で暗号化する第 2 の暗号化手段をさらに備えるようにすることができる。

- 5 第 1 の暗号化手段および第 2 の暗号化手段のうちの一方は、記録媒体の ID と記録媒体鍵を作用させてコンテンツを暗号化するようにすることができる。

本発明の入力方法は、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号

- 10 化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

本発明の第 2 の記録媒体のプログラムは、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

- 15 本発明の第 2 のプログラムは、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

- 20 本発明の再生システムは、再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、再生手段により再生された保護情報に基づいて、バス上の出力装置へのコンテンツの送出を制御する送出制御手段とを備え、出力装置は、送出制御手段により送出されたコンテンツを外部に出力する出力手段を備えることを特徴とする。
- 25

保護情報は、コンテンツの所定の単位ごとに記録されているようにすることができる。

所定の単位は、2048バイトであるようにすることができる。

再生装置は、再生手段により再生されたコンテンツを復号する復号手段をさらに備えるようにすることができる。

再生装置は、バス上の装置を認証する認証手段をさらに備えるようにすることができる。

再生装置は、保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段によりバス上の出力装置が認証されている場合、バスへのコンテンツの送出前に、コンテンツを暗号化する暗号化手段をさらに備え、出力装置は、暗号化手段により暗号化されたコンテンツを復号する第1の復号手段をさらに備えるようにすることができる。

出力装置は、第1の復号手段により復号されたコンテンツを、記録媒体のIDと記録媒体鍵を作用させて復号する第2の復号手段をさらに備えるようにすることができる。

保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段によりバス上の装置が認証されていない場合、送出制御手段は、バス上の装置へのコンテンツの送出を禁止するようにすることができる。

本発明の第1の再生方法は、再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生し、再生された保護情報に基づいて、バス上の出力装置へのコンテンツの送出を制御し、出力装置は、再生装置から送出されたコンテンツを外部に出力することを特徴とする。

本発明の再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、再生手段により再生された保護情報に基づいて、バスを介しての他の装

置へのコンテンツの出力を制御する出力制御手段とを備えることを特徴とする。

保護情報は、コンテンツの所定の単位ごとに記録されているようにすることができる。

所定の単位は、2048バイトであるようにすることができる。

- 5      他の装置を認証する認証手段と、コンテンツを暗号化する暗号化手段とをさらに備え、保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段により他の装置が認証されている場合、暗号化手段は、バスへのコンテンツの送出前に、コンテンツを暗号化するようにすることができる。

- 10     保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段により他の装置が認証されていない場合、出力制御手段は、バスへのコンテンツの出力を禁止するようにすることができる。

- 15     本発明の第2の再生方法は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

- 20     本発明の第3の記録媒体のプログラムは、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

- 25     本発明の第3のプログラムは、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

第1の本発明においては、入力装置により、入力されたコンテンツを保護するか否かが判断され、判断された結果に基づいて、記録装置により、コンテンツがバス上での伝送において保護すべきコンテンツであるか否かを示す保護情報が、コンテンツとともに記録媒体に記録される。

- 5     入力装置は、独立した装置であっても良いし、入力記録装置の入力処理を行うブロックであってもよい。

記録装置は、独立した装置であっても良いし、記録再生装置の記録処理を行うブロックであってもよい。

- 10    第2の本発明においては、バスを介して接続された他の装置と相互に認証が行われる。そして、他の装置からバスを介して供給される暗号化されたコンテンツが復号され、復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報が、記録媒体に記録される。

- 15    第3の本発明においては、バスを介して接続された記録装置と相互に認証が行われる。そして、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツが暗号化され、暗号化されたコンテンツが、バスを介して記録装置に供給される。

- 20    第4の本発明においては、再生装置により、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報が再生され、再生された保護情報に基づいて、バス上の出力装置へのコンテンツの送出が制御される。そして、出力装置により、再生装置から送出されたコンテンツが外部に出力される。

再生装置は、独立した装置であっても良いし、記録再生装置の再生処理を行うブロックであってもよい。

- 25    出力装置は、独立した装置であっても良いし、再生出力装置の出力処理を行うブロックであってもよい。

第5の本発明においては、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報が再生され、

再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力が制御される。

#### 図面の簡単な説明

- 5 図 1 は、従来の記録再生装置の構成例を示すブロック図である。  
図 2 は、従来の記録再生装置の他の構成例を示すブロック図である。  
図 3 は、従来の記録再生装置のさらに他の構成例を示すブロック図である。  
図 4 は、本発明を適用した記録再生装置の構成例を示すブロック図である。  
図 5 は、本発明のデータフォーマットの構成例を示す図である。
- 10 図 6 は、図 5 のデータフレームの構成例を示す図である。  
図 7 は、図 5 のスクランブルデータフレームの構成例を示す図である。  
図 8 は、図 5 のユーザコントロールデータの構成例を示す図である。  
図 9 は、図 4 のコンテンツ保護部 132 の構成例を示すブロック図である。  
図 10 は、本発明のディスク鍵について説明するツリー構造図である。
- 15 図 11A は、本発明のディスク鍵に使用される RKB の例を説明する図である。  
図 11B は、本発明のディスク鍵に使用される RKB の例を説明する図である。  
図 12 は、図 11A および図 11B の RKB の使用例を説明する図である。  
図 13 は、図 4 の AV ボードの相互認証処理を説明するフローチャートである。  
図 14 は、図 4 のドライブの相互認証処理を説明するフローチャートである。
- 20 図 15 は、図 4 の AV ボードの記録要求処理を説明するフローチャートである。  
図 16 は、図 15 のステップ S103 のブロック鍵生成処理を説明するフローチャートである。  
図 17 は、図 16 の処理に対応する図 4 のドライブのディスク情報再生処理を説明するフローチャートである。
- 25 図 18 は、図 4 のドライブの記録処理を説明するフローチャートである。  
図 19 は、図 4 のドライブの再生処理を説明するフローチャートである。  
図 20 は、図 4 の AV ボードの再生処理を説明するフローチャートである。

図 2 1 は、図 4 の記録再生装置の他の構成例を示すブロック図である。

図 2 2 は、図 2 1 のドライブの記録処理を説明するフローチャートである。

図 2 3 は、図 2 1 のドライブの再生処理を説明するフローチャートである。

図 2 4 は、本発明の記録再生装置の他の構成例を示すブロック図である。

5 図 2 5 は、図 2 4 のコンテンツ保護部 4 1 1 の構成例を示すブロック図である。

図 2 6 は、図 2 4 のドライブのブロック鍵生成処理を説明するフローチャートである。

図 2 7 は、図 2 4 の A V ボードの記録要求処理を説明するフローチャートである。

10 図 2 8 は、図 2 4 のドライブの記録処理を説明するフローチャートである。

図 2 9 は、図 2 4 のドライブの再生処理を説明するフローチャートである。

図 3 0 は、図 2 4 の A V ボードの再生処理を説明するフローチャートである。

図 3 1 は、図 2 4 の記録再生装置の他の構成例を示すブロック図である。

図 3 2 は、図 3 1 のドライブの記録処理を説明するフローチャートである。

15 図 3 3 は、図 3 1 のドライブの再生処理を説明するフローチャートである。

図 3 4 は、本発明の記録再生装置の他の構成例を示すブロック図である。

#### 発明を実施するための最良の形態

以下、図を参照して本発明の実施の形態について説明する。

20 図 4 は、本発明を適用した記録再生装置 1 0 1 の構成例を表している。家庭内 LAN (Local Area Network) に代表されるバス 1 1 3 には、ドライブ 1 1 1、A V ボード 1 1 2、および HDD (hard disk drive) 1 1 4 が接続されている。なお、ドライブ 1 1 1、A V ボード 1 1 2、および HDD 1 1 4 は、独立に販売されるものであり、ユーザにより、バス 1 1 3 に接続されるものである。

25 この例の場合、ドライブ 1 1 1 および A V ボード 1 1 2 は、それぞれ自分自身の秘密鍵と公開鍵を有している。この公開鍵および秘密鍵の登録は、例えば、メーカーにより出荷時に、あらかじめ行なわれている。なお、公開鍵は、図示せぬ認

証局が発行した電子署名の中に記憶される。ドライブ 1 1 1 および A V ボード 1 1 2 の間におけるコンテンツの転送には、例えば、RSA などの公開鍵暗号化方式が使用される。なお、秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。

- 5      ドライブ 1 1 1 は、他の装置（図 4 の例の場合、A V ボード 1 1 2）との相互認証処理を実行する相互認証部 1 2 1、ドライブ 1 1 1 の各部の制御を実行する入出力制御部 1 2 2、および、ドライブ 1 1 1 に装着された光ディスク 1 4 1 に、コンテンツの記録または再生を実行する記録再生処理部 1 2 3 により構成される。

- 10      A V ボード 1 1 2 は、他の装置（図 4 の例の場合、ドライブ 1 1 1）との相互認証処理を実行する相互認証部 1 3 1、光ディスク 1 4 1 に記憶するコンテンツを暗号化するコンテンツ保護部 1 3 2、アンテナなどにより構成される入力部 1 3 4 を介してコンテンツを受信したり、コンテンツをデコードし、出力部 1 3 5 に出力する A V コンテンツ処理部 1 3 3 により構成される。

- 15      ドライブ 1 1 1 の相互認証部 1 2 1 は、A V ボード 1 1 2 の相互認証部 1 3 1 との間で相互認証処理を実行する。具体的に説明すると、ドライブ 1 1 1 と A V ボード 1 1 2 が接続され、それぞれの電源がオンされたとき、A V ボード 1 1 2 の相互認証部 1 3 1 は、内蔵する乱数発生部（図示せず）の乱数に基づいて、共通鍵を生成し、生成された共通鍵をドライブ 1 1 1 の公開鍵で暗号化し、A V ボード 1 1 2 の秘密鍵により暗号化された共通鍵への署名を生成する。また、相互  
20      認証部 1 3 1 は、内蔵するメモリから、認証局から予め取得され、記憶されている A V ボード電子証明書を読み出し、暗号化された共通鍵、A V ボード 1 1 2 による共通鍵への署名、および A V ボード電子証明書を、バス 1 1 3 を介して、ドライブ 1 1 1 に送信する。

- 25      ドライブ 1 1 1 の相互認証部 1 2 1 は、これらを受信し、暗号化された共通鍵をドライブ 1 1 1 の秘密鍵で復号して共通鍵（第 1 の共通鍵）を取得するとともに、A V ボード電子証明書を、認証局から予め取得された認証局公開鍵で復号し、A V ボード 1 1 2 が正当な A V ボードであることを確認する。また、相互認証部

1 2 1 は、復号された A V ボード電子証明書から取得された A V ボード 1 1 2 の公開鍵により、共通鍵への署名を復号して共通鍵（第 2 の共通鍵）を取得する。ドライブ 1 1 1 の相互認証部 1 2 1 は、第 1 の共通鍵と第 2 の共通鍵を比較し、両者が等しいと判断された場合、バス 1 1 3 上で、共通鍵が改ざんされていないと判断する。これにより、共通鍵が、ドライブ 1 1 1 と A V ボード 1 1 2 との間で共有されたことになる。

10 以上のようにして、ドライブ 1 1 1 の相互認証部 1 2 1 は、A V ボード 1 1 2 の相互認証部 1 3 1 との間で相互認証処理を実行し、A V ボード 1 1 2 を相互認証する。これにより、相互認証部 1 2 1 および相互認証部 1 3 1 は、お互いに、この共通鍵を用いて、コンテンツを暗号化して送信したり、受信したコンテンツを復号することができる。

15 一方、HDD 1 1 4 は、A V ボード 1 1 2 の相互認証部 1 3 1 のような相互認証機能を有していない。したがって、HDD 1 1 4 は、バス 1 1 3 上に流れても問題がない（保護しなくてもよい）フリーコンテンツ（保護する必要がないコンテンツ）の送受信をドライブ 1 1 1 と実行することができる。

20 A V ボード 1 1 2 の A V コンテンツ処理部 1 3 3 は、入力部 1 3 4 を介して放送信号（暗号化またはスクランブルされているコンテンツに対応する信号）を受信すると、予め記憶されている鍵（放送信号を送信する機器と共有している鍵）で暗号化またはスクランブルされているコンテンツを復号し、コンテンツ保護部 1 3 2 に供給する。

25 また、A V コンテンツ処理部 1 3 3 は、入力されたコンテンツが、暗号化またはスクランブルされているか否かに基づいて、入力されたコンテンツが保護すべきコンテンツであるか否かという判断を実行することができる。なお、このコンテンツ（放送信号）に、例えば、コンテンツのコピーを制限するために、「Copy Free(コピー可)」, 「Copy Once(一世代のみコピー可)」, 「No More Copy(この世代以上のコピー不可)」, 「Copy Prohibited(コピー禁止)」というコピー世代管理情報(Copy generation management information)を示す、例えば、



C G M S (Copy Generation Management System) 信号のような C C I (Copy Control Information) が付加されている場合、このコピー世代管理情報が「Copy Free」のときには、入力されたコンテンツが保護すべきコンテンツではないとし、「Copy Once」, 「No More Copy」または「Copy Prohibited」のときには、  
5 入力されたコンテンツが保護すべきコンテンツであると判断するようにしてもよい。

コンテンツ保護部 1 3 2 は、コンテンツを A V コンテンツ処理部 1 3 3 より入力し、A V コンテンツ処理部 1 3 3 によりそのコンテンツが保護すべきコンテンツであると判断された場合、相互認証部 1 3 1 より供給された光ディスク 1 4 1  
10 の R K B を作用させたディスク鍵を取得し、取得されたディスク鍵および光ディスク 1 4 1 のディスク I D に基づいて、ブロック鍵を生成する。コンテンツ保護部 1 3 2 は、このブロック鍵を用いて、光ディスク 1 4 1 上におけるコンテンツ保護のために、保護すべきコンテンツを暗号化し、相互認証部 1 3 1 に供給する。

相互認証部 1 3 1 は、コンテンツ保護部 1 3 2 により暗号化されたコンテンツ  
15 を、バス 1 1 3 上におけるコンテンツ保護のために、ドライブ 1 1 1 との共通鍵で暗号化し、バス 1 1 3 を介してドライブ 1 1 1 に出力する。

なお、A V コンテンツ処理部 1 3 3 によりコンテンツが保護すべきコンテンツではないと判断された場合、コンテンツ保護部 1 3 2 および相互認証部 1 3 1 は、そのコンテンツを暗号化せず、バス 1 1 3 を介してドライブ 1 1 1 に出力する。

20 ドライブ 1 1 1 の相互認証部 1 2 1 は、バス 1 1 3 を介して A V ボード 1 1 2 からコンテンツを入力する。また、相互認証部 1 2 1 は、入力されたコンテンツが暗号化されている場合、ドライブ 1 1 1 との共通鍵で復号し、復号したコンテンツを記録再生処理部 1 2 3 に供給する。

入出力制御部 1 2 2 は、相互認証部 1 2 1 に入力されたコンテンツが、A V ボード 1 1 2 の相互認証部 1 3 1 により、A V ボード 1 1 2 との共通鍵で暗号化されているか否か（すなわち、A V コンテンツ処理部 1 3 3 により保護すべきコンテンツであると判断されたか否か）に基づいて、そのコンテンツがバス 1 1 3 上  
25

で保護されるべきコンテンツであるか否かを判断する。そして、入出力制御部 1 2 2 は、入力されたコンテンツがバス 1 1 3 上で保護されるべきコンテンツであるか否か、かつ、相互認証部 1 2 1 により A V ボード 1 1 2 との間で相互認証がされたか否かに基づいて、記録再生処理部 1 2 3 によるコンテンツの記録制御を行う。

また、入出力制御部 1 2 2 は、入力されたコンテンツが保護されるべきコンテンツであるか否か、かつ、相互認証部 1 2 1 により A V ボード 1 1 2 との間で相互認証がされたか否かに基づいて、記録再生処理部 1 2 3 を制御し、光ディスク 1 4 1 に記録されているディスク I D および R K B (Renewal Key Block) などの光ディスク 1 4 1 のディスク情報を再生させる。

記録再生処理部 1 2 3 は、光ディスク 1 4 1 にコンテンツを記録する場合、入出力制御部 1 2 2 の指示に基づいて、記録するコンテンツが、バス 1 1 3 上で保護すべきコンテンツまたはバス 1 1 3 上で保護不要のコンテンツであることを示す保護情報を生成し、その保護情報をコンテンツとともに光ディスク 1 4 1 に記録する。

図 5 は、光ディスク 1 4 1 に記録されるデータフォーマットの構成例を示している。

このデータフォーマットにおいては、1 フレーム当り 2 K (2 0 4 8) バイトで 3 2 フレームのユーザデータ 2 0 1 と、1 フレーム当り 1 8 バイトで 3 2 フレームのユーザコントロールデータ 2 0 2 により、3 2 セクタが構成されている。

ユーザデータ 2 0 1 は、コンテンツのデータなどにより構成される。このユーザデータ 2 0 1 は、各フレームに、4 つ (4 バイト) の E D C (エラー検出コード) が付加され、図 6 に示されるようなデータフレーム 2 0 3 が構成される。

図 6 の例においては、1 つのデータフレームは、2 0 5 2 バイトで構成される。すなわち、1 つのデータフレームは、U d 0 乃至 U d 2 0 4 7 の番号が振られた 2 0 4 8 個のユーザデータバイト、および e d 2 0 4 8 乃至 e d 2 0 5 1 の番号が振られた 4 つの E D C により構成されている。

このデータフレーム 203 が 32 フレーム分集められ、 $16 \times 9$  バイトに配列された物理アドレス 204 に基づいて、図 7 に示されるようなスクランブルデータフレーム 205 として構成される。

図 7 の例の場合、1 番目の（図中、左端の列の）フレームは、 $d(0, 0)$  ,  
 5  $d(1, 0)$  ,  $\dots$  ,  $d(2051, 0)$  の番号が振られた 2052 バイトにより構成され、2 番目（図中、左端から 2 番目の列の）のフレームは、 $d(0, 1)$  ,  
 $d(1, 1)$  ,  $\dots$  ,  $d(2051, 1)$  の番号が振られた 2052 バイトにより構成される。同様に、 $F-1$  番目のフレームは、 $d(0, F)$  ,  $d(1, F)$  ,  
 $\dots$  ,  $d(2051, F)$  の番号が振られた 2052 バイトにより構成され、32  
 10 番目の（図中、右端の列の）フレームは、 $d(0, 31)$  ,  $d(1, 31)$  ,  $\dots$  ,  
 $d(2051, 31)$  の番号が振られた 2052 バイトにより構成される。

以上のようなスクランブルデータフレーム 205 から、216 行 304 列のデータブロック 206 が形成される。データブロック 206 に、32 行のパリティを付加することにより、LDC（長距離コード：誤り訂正）ブロック 207 が形  
 15 成される。LDC ブロック 207 から、152 列 496 行の LDC クラスタ 208 が形成される。LDC クラスタ 208 は、それぞれが 38 列の 4 つの LDC 列  
 $209-1$  乃至  $209-4$  に分割され、後述する BIS 列  $213-1$  乃至  $213-3$  とにより ECC クラスタ 221 を構成する。

一方、この記録再生装置 101 により付加されるアドレスおよび制御データを  
 20 説明する。ユーザコントロールデータ（論理アドレスおよび制御データ）202 は、図 8 に示されるように、 $32 \times 18$  バイトに配列される。

図 8 の例の場合、1 番目の（図中、左端の列の）フレームは、 $UC(0, 0)$  ,  
 $UC(1, 0)$  ,  $\dots$  ,  $UC(17, 0)$  の番号が振られた 18 バイトにより構成され、2 番目の（図中、左端から 2 番目の列の）フレームは、 $UC(0, 1)$  ,  
 25  $UC(1, 1)$  ,  $\dots$  ,  $UC(17, 1)$  の番号が振られた 18 バイトにより構成される。同様に、 $S-1$  番目のフレームは、 $UC(0, S)$  ,  $UC(1, S)$  ,  
 $\dots$  ,  $UC(17, S)$  の番号が振られた 18 バイトにより構成され、32 番目の

(図中、右端の列の) フレームは、UC (0, 31), UC (1, 31), ..., UC (17, 31) の番号が振られた 2052 バイトにより構成される。

上述したように、このデータフォーマットにおいては、各フレーム単位で、2 K (2048) バイトのユーザデータ 201 につき、18 バイトのユーザコントロールデータ 202 が対応している。そこで、このユーザデータ 201 (2 K バイト) に記録されるデータ (コンテンツ) に対して、バス 113 上で保護すべきコンテンツであるか否かを示す保護情報が生成され、そのユーザデータ 201 に対応するユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットに格納される。

- 10     例えば、記録するコンテンツがバス 113 上で保護すべきコンテンツである場合、保護情報として、ユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットに、「0」が生成され、記録される。また、記録するコンテンツがバス 113 上で保護する必要がないコンテンツである場合、保護情報として、ユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットに、「1」が生成され、記録される。なお、既存のデータフォーマットにおいては、ユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットには、もともと「0」が格納されている (未使用とされている)。したがって、既存のデータフォーマットにより記録した保護すべきコンテンツに対しても、バス 113 上で保護すべき情報が格納されていることになるので、既存のものとの互換性を保持することができる。

- 25     保護を要するコンテンツの保護情報を「1」とし、保護不要のコンテンツの保護情報を「0」とすることも可能である。しかしながら、そのようにすると、既存のコンテンツはすべてバス 113 上で保護不要のコンテンツとなってしまう、実質的に保護することができなくなってしまう。そこで、保護を要するコンテンツの保護情報を「0」とし、保護不要のコンテンツの保護情報を「1」とするのが好ましい。

また、物理アドレス 204 は、16 × 9 バイトに配列される。この物理アドレ

ス 2 0 4 は、ディスク 1 4 1 上の物理的距離に関係する。

3 2 × 1 8 バイトのユーザコントロールデータ 2 0 2 から、物理アドレス 2 0 4 に基づいて、2 4 列 × 3 0 行のアクセスブロック 2 1 0 が形成される。アクセスブロック 2 1 0 は、3 2 行のパリティが付加され、B I S (バースト指示サブ  
5 コード) ブロック 2 1 1 が形成される。B I S ブロック 2 1 1 は、3 列 × 4 9 6 行の B I S クラスタ 2 1 2 に配列される。

B I S クラスタ 2 1 2 は、L D C 列 2 0 9 - 1 乃至 2 0 9 - 4 の間に、それぞれが 1 列の 3 つの B I S 列 2 1 3 - 1 乃至 2 1 3 - 3 に充填され、1 5 5 列 × 4 9 6 行の E C C クラスタ 2 2 1 が形成される。この E C C クラスタ 2 2 1 から、  
10 4 5 チャンネルビットのデータ (data) および 1 チャンネルビットのコントロールデータ (dc contr.) の 4 2 個の組み合わせにより物理クラスタ 2 2 2 が形成され、光ディスク 1 4 1 に記録される。

この物理クラスタ 2 2 2 は、1 9 3 2 チャンネルビット (1 2 8 8 データビット) の 4 9 6 の記録フレームにグループ化されている。なお、物理クラスタ 2 2  
15 2 の最初のデータ (data) のうち、2 0 チャンネルビットは、同期ビット群 (Frame Sync) とされる。

以上のようにして、記録再生処理部 1 2 3 により、記録するコンテンツがバス 1 1 3 上で保護すべきコンテンツである場合、保護情報として、「0」が生成 (格納) され、記録するコンテンツがバス 1 1 3 上で保護不要のコンテンツである  
20 場合、保護情報として、「1」が生成 (格納) され、生成された保護情報がユーザコントロールデータ 2 0 2 に記録される。

このデータフォーマットの光ディスク 1 4 1 に記録されたコンテンツを再生する場合の誤り訂正動作としては、一般的には、B I S の誤り訂正動作を行い、B I S の誤り訂正動作の結果を L D C の誤り訂正動作を行う際の消失情報として用  
25 いる。したがって、L D C の誤り訂正動作が終わって、ユーザデータを出力できるようになる前に、B I S の誤り訂正動作は終了しているため、B I S に含まれるユーザコントロールデータは、すでに得られている。したがって、ユーザコン

トロールデータを用いて、ユーザデータの出力制御は可能である。

以上のように、光ディスク 1 4 1 に記録された保護情報は、記録再生処理部 1 2 3 により、光ディスク 1 4 1 に記録されたコンテンツを再生する場合、コンテンツよりも先に再生されるので、この再生された保護情報に基づいて、入出力制

5 御部 1 2 2 は、バス 1 1 3 へのコンテンツの出力の制御を行う。

例えば、入出力制御部 1 2 2 は、相互認証部 1 2 1 により A V ボード 1 1 2 との間で相互認証がされたか否か、および、再生されたコンテンツがバス 1 1 3 上で保護されるべきコンテンツであるか（保護情報が「0」であるか）否かに基づいて、相互認証部 1 2 1 によるコンテンツのバス 1 1 3 への出力制御を行う。相

10 互認証部 1 2 1 は、この入出力制御部 1 2 2 の制御に基づいて、再生されたコンテンツを、ドライブ 1 1 1 との共通鍵で暗号化し、バス 1 1 3 を介して A V ボード 1 1 2 に出力する。

このドライブ 1 1 1 の相互認証部 1 2 1 により暗号化されたコンテンツが入力されると、A V ボード 1 1 2 の相互認証部 1 3 1 は、そのコンテンツを復号し、

15 コンテンツ保護部 1 3 2 に供給する。

コンテンツ保護部 1 3 2 は、相互認証部 1 3 1 により A V ボード 1 1 2 との共通鍵を用いて復号されたコンテンツを、さらに、光ディスク 1 4 1 のディスク I D およびディスク鍵を作用させたブロック鍵により復号し、A V コンテンツ処理部 1 3 3 に供給する。A V コンテンツ処理部 1 3 3 は、復号されたコンテンツを、

20 例えば、MPEG (Moving Picture Experts Group) 方式でデコードし、再生する。出力部 1 3 5 は、再生されたコンテンツを出力する。

以上のように、A V ボード 1 1 2 は、ドライブ 1 1 1 と相互認証されているので、著作権などにより保護されるべきコンテンツ（保護すべきコンテンツ）または保護不要のコンテンツをお互いに送受信することができる。

25 一方、例えば、HDD 1 1 4 により保護されるべきコンテンツがドライブ 1 1 1 に送信されてきたとしても、HDD 1 1 4 は、ドライブ 1 1 1 により相互認証されないで、そのコンテンツは、保護不要のコンテンツであればドライブ 1 1

1で処理される。すなわち、この記録再生装置101において、コピーフリーのコンテンツのみを扱う相互認証しないデータの記録は許可される。

以上のようにして、この記録再生装置101においては、著作権などによりコンテンツの保護が必要か否かによって、コンテンツの暗号化またはコンテンツの汎用バスへの出力が柔軟に制御される。

図9は、コンテンツ保護部132の構成例を示している。なお、図9においては、説明の便宜上、コンテンツ保護部132と光ディスク141しか記載されていないが、実際には、コンテンツ保護部132と光ディスク141との間では、図4に示されるように、相互認証部131、バス113、相互認証部121および記録再生処理部123が、それぞれの処理を実行している。

図9の例においては、コンテンツ保護部132は、RKB処理部252、鍵生成部253および暗号化部254により構成される。

RKB処理部252は、AVコンテンツ処理部133からの入力されたコンテンツが保護されるべきコンテンツであるか否かの情報に基づいて、光ディスク141から供給されたRKB、コンテンツ保護部132に予め記憶されているデバイスIDおよびデバイス鍵を作用させて、ディスク鍵を取得する（このディスク鍵の取得処理については、特開2002-84271号公報に開示されており、さらに、図10乃至図12を参照して詳しく後述する）。

鍵生成部253は、RKB処理部252により取得されたディスク鍵、光ディスク141から供給されたディスクID、および、コンテンツ保護部132に記憶されている記録情報（例えば、ブロックシード、タイトルキーまたは記録モードなどの記録時に使用する情報）を作用させて、ブロック鍵を生成する。

暗号化部254は、光ディスク141より供給されるコンテンツが暗号化されている場合、鍵生成部253により生成されたブロック鍵を用いて、暗号化コンテンツを復号し、AVコンテンツ処理部133に出力する。暗号化部254は、光ディスク141より供給されるコンテンツが暗号化されていない場合、そのコンテンツをそのまま、AVコンテンツ処理部133に出力する。

また、暗号化部 2 5 4 は、A V コンテンツ処理部 1 3 3 からの入力されたコンテンツが保護されるべきコンテンツであるか否かの情報に基づいて、A V コンテンツ処理部 1 3 3 より供給されるコンテンツが保護すべきコンテンツである場合、光ディスク 1 4 1 上でのコンテンツ保護のために、鍵生成部 2 5 3 により生成されたブロック鍵を用いて、コンテンツを暗号化し、光ディスク 1 4 1 に供給する。暗号化部 2 5 4 は、A V コンテンツ処理部 1 3 3 より供給されるコンテンツが保護不要のコンテンツである場合、コンテンツをそのまま（暗号化せずに）、光ディスク 1 4 1 に供給する。

次に、ディスク鍵の取得処理に使用される R K B について詳しく説明する。図 1 0 は、本発明の記録再生装置 1 0 1 の鍵の配布構成を示す図である。図 1 0 の最下段に示すナンバー 0 乃至 1 5 が個々の記録再生装置（デバイス）に対応する。すなわち、図 1 0 に示される木（ツリー）構造の各葉（リーフ：leaf）がそれぞれ記録再生装置に相当する。

各デバイス 0 乃至 1 5 は、製造時（出荷時）に、予め設定されている初期ツリーにおける、自分のリーフからルート（最上段）に至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図 1 0 の最下段に示す K 0 0 0 0 乃至 K 1 1 1 1 が、各デバイス 0 乃至 1 5 にそれぞれ割り当てられたリーフキーであり、最上段の K R から、最下段から 2 番目の節（ノード）に記載されたキー K R 乃至 K 1 1 1 1 がノードキーである。

図 1 0 の例においては、例えば、デバイス 0 は、リーフキー K 0 0 0 0 と、ノードキー K 0 0 0, K 0 0, K 0, K R を所有する。デバイス 5 は、K 0 1 0 1, K 0 1 0, K 0 1, K 0, K R を所有する。デバイス 1 5 は、K 1 1 1 1, K 1 1 1, K 1 1, K 1, K R を所有する。なお、図 1 0 のツリーには、デバイスが 1 6 個のみ記載され、ツリー構造も 4 段構成の均衡のとれた左右対称構成として示されているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を有するようにしてもよい。

また、図 1 0 のツリー構造に含まれる各記録再生装置には、様々な記録媒体、



例えば、DVD、CD、MD（商標）、メモリスティック（登録商標）などを使用する様々なタイプの記録再生装置が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に、図10に示されるようなキー配布構成が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば、図10の点線で囲まれた部分、すなわち、デバイス0, 1, 2, 3は、同一の記録媒体を用いる1つのグループとして設定される。このツリー構造においては、1つのグループに含まれる4つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00, K0, KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスター鍵をデバイス0, 1, 2, 3のみに提供することが可能となる。

例えば、共通に保有するノードキーK00自体をマスター鍵として設定すれば、新たな鍵送付を実行することなく、デバイス0, 1, 2, 3のみに共通のマスター鍵の設定が可能である。また、新たなマスター鍵KmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスター鍵Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

また、ある時点tにおいて、デバイス3の所有する鍵K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキーK001, K00, K0, KRをそれぞれ新たな鍵：K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1,

2にその更新キーを伝える必要がある。ここで、 $K(t) a a a$ は、鍵 $K a a a$ の世代 (Generation) :  $t$ の更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図11Aに示すRKB (Renewal Key Block) と呼ばれるブロックデータによって構成される  
5 テーブルを、たとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。

図11Aに示すRKBには、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図11Aは、図10に示されるツリー構造中のデバイス0, 1, 2において、世代 $t$ の更新ノードキー  
10 を配布することを目的として形成されたブロックデータの例を示す。上述したように、デバイス0, デバイス1は、更新ノードキーとして $K(t) 0 0$ ,  $K(t) 0$ ,  $K(t) R$ が必要であり、デバイス2は、更新ノードキーとして $K(t) 0 0 1$ ,  $K(t) 0 0$ ,  $K(t) 0$ ,  $K(t) R$ が必要である。

図11AのRKBに示されるように、RKBには複数の暗号化キーが含まれる。  
15 最下段の暗号化キーは、 $Enc(K 0 0 1 0, K(t) 0 0 1)$ である。これはデバイス2の持つリーフキー $K 0 0 1 0$ によって暗号化された更新ノードキー $K(t) 0 0 1$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t) 0 0 1$ を得ることができる。また、復号により得た $K(t) 0 0 1$ を用いて、図11Aの下から2段目の暗号化キー $Enc(K(t) 0 0 1, K(t) 0 0)$ が復号可能となり、更新ノードキー $K(t) 0 0$ を得ることができる。以下、順次、図11Aの上から2段目の暗号化キー $Enc(K(t) 0 0, K(t) 0)$ を復号し、更新ノードキー $K(t) 0$ 、図11Aの上から1段目の暗号化キー $Enc(K(t) 0, K(t) R)$ を復号し、 $K(t) R$ が得られる。  
20

25 一方、ノードキー $K 0 0 0$ は更新する対象に含まれておらず、デバイス0, 1が、更新ノードキーとして必要とするのは、 $K(t) 0 0$ ,  $K(t) 0$ ,  $K(t) R$ である。デバイス0, 1は、図11Aの上から3段目の暗号化キー $Enc$

c (K 0 0 0, K (t) 0 0) を復号し、K (t) 0 0 を取得し、以下、図 1 1 A の上から 2 段目の暗号化キー E n c (K (t) 0 0, K (t) 0) を復号し、更新ノードキー K (t) 0 を得、図 1 1 A の上から 1 段目の暗号化キー E n c (K (t) 0, K (t) R) を復号し、K (t) R を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 K (t) R を得ることができる。なお、図 1 1 A のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図 1 0 に示すツリー構造の上位 2 段のノードキー K 0, K R の更新が不要であり、ノードキー K 0 0 のみの更新処理が必要である場合には、図 1 1 B の R K B を用いることで、更新ノードキー K (t) 0 0 をデバイス 0, 1, 2 に配布することができる。

図 1 1 B に示す R K B は、例えば、特定のグループにおいて共有する新たなマスター鍵を配布する場合に利用可能である。具体例として、図 1 0 に、点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のマスター鍵 K (t) master が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K 0 0 を更新した K (t) 0 0 を用いて新たな共通の更新マスター鍵 K (t) master を暗号化したデータ E n c (K (t), K (t) master) を、図 1 1 B に示す R K B とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス 0, 1, 2, 3 は R K B を処理して得た K (t) 0 0 を用いて上記暗号文を復号すれば、t 時点でのマスター鍵 K (t) master を得ることが可能になる。

以上においては、R K B を用いて、各記録再生装置に対してマスター鍵を伝送し、これを用いて記録再生装置がデータの記録、再生を行う例を説明したが、本発明においては、上述したマスター鍵として、記録媒体のみに限定されたものであるディスク鍵が使用される。このディスク鍵は、図 1 2 に示されるように、記

録媒体のRKB (Renewal Key Block)を用いて生成される。なお、ディスク鍵K(t) media は、マスター鍵をその記録媒体のみに限定したものであり、基本的な構成は、上述したマスター鍵と同様であるため、その説明を省略する。

図12の例の場合、デバイス0が、記録媒体に格納されている世代:t時点の  
5 RKBと、自分があらかじめ格納しているリーフキーK0000と、ノードキーK000, K00を用いて更新ノードキーK(t)00を生成し、それを用いて更新ディスク鍵K(t) media を得る様子を示している。ここで得たK(t) media は、その記録媒体のデータの記録、再生時に使用される。

なお、図12におけるプレ記録世代番号(Generation #n)は、ディスク鍵に  
10 おいてはマスター鍵のように世代の新旧という概念はないので必須ではなくオプションとして設定される。

以上のようにして、光ディスク141からのRKB、コンテンツ保護部132のデバイスID(例えば、図10のデバイス0)、デバイス鍵(例えば、図10のデバイス0におけるリーフキーK0000)およびノードキー(図10のデバイス0におけるK000, K00, ...)などに基づいて、ディスク鍵が取得される。このディスク鍵の取得処理は、例えば、コンテンツの記録もしくは再生のために、光ディスク141が記録再生装置101のドライブ111に装着された際に実行されるようにしてもよいし、または、光ディスク141が装着されており、コンテンツの記録もしくは再生を指示した際に実行されるようにしてもよい。

20 次に、図13のフローチャートを参照して、記録再生装置101のAVボード112の相互認証処理について説明する。

ドライブ111とAVボード112が接続され、それぞれの電源がオンされたとき、ステップS11において、AVボード112の相互認証部131は、内蔵する乱数発生部の乱数に基づいて、共通鍵を生成する。ステップS12において、  
25 相互認証部131は、生成された共通鍵をドライブ111の公開鍵で暗号化する。ステップS13において、相互認証部131は、AVボード112の秘密鍵により暗号化された共通鍵への署名を生成する。ステップS14において、相互認証

部 1 3 1 は、内蔵するメモリより、図示せぬ認証局から予め取得され、記憶されている A V ボード電子証明書を読み出す。ステップ S 1 5 において、相互認証部 1 3 1 は、暗号化された共通鍵、A V ボード 1 1 2 による共通鍵への署名、および A V ボード電子証明書を、バス 1 1 3 を介して、ドライブ 1 1 1 に送信する。

- 5      このようにして、A V ボード 1 1 2 から、暗号化された共通鍵、A V ボード 1 1 2 による共通鍵への署名、および A V ボード電子証明書がドライブ 1 1 1 に送信される。この A V ボード 1 1 2 の相互認証処理に対応するドライブ 1 1 1 の相互認証処理を、図 1 4 のフローチャートを参照して説明する。

- ステップ S 3 1 において、ドライブ 1 1 1 の相互認証部 1 2 1 は、受信した A  
10   V ボード電子証明書を、予め取得してあるか、その都度取得する認証局公開鍵に基づいて復号する。ステップ S 3 2 において、相互認証部 1 2 1 は、ステップ S 3 1 において復号された A V ボード電子証明書に基づいて、A V ボード 1 1 2 が正当な A V ボードであるか否かを判断する。A V ボード電子証明書が復号できなかったり、改ざんされている場合には、ステップ S 3 2 において、A V ボード 1  
15   1 2 が正当な A V ボードではないと判断され、処理は終了する。

- ステップ S 3 2 において、A V ボード 1 1 2 が正当な A V ボードであると判断された場合、A V ボード電子証明書を復号することにより A V ボード 1 1 2 の公開鍵が得られる。相互認証部 1 2 1 は、ステップ S 3 3 において、暗号化されている共通鍵を、ドライブ 1 1 1 の秘密鍵を用いて復号する。ステップ S 3 4 にお  
20   いて、相互認証部 1 2 1 は、A V ボード 1 1 2 による共通鍵への署名を、A V ボード 1 1 2 の公開鍵を用いて復号する。

- ステップ S 3 5 において、相互認証部 1 2 1 は、ステップ S 3 3 において復号された共通鍵と、署名に平文で添付されている共通鍵を比較し、両者が一致するか否かを判断する。これにより、その共通鍵が正当な共通鍵であるか否かが判定  
25   される。ステップ S 3 5 において、共通鍵と、署名の共通鍵が一致すると判断された場合、相互認証部 1 2 1 は、A V ボード 1 1 2 から正当な共通鍵が送信されてきたと判定し、ステップ S 3 6 において、共通鍵を記憶する。一方、ステップ

S 3 5において、共通鍵と、署名の共通鍵が一致しないと判断された場合、相互認証部 1 2 1 は、A V ボード 1 1 2 とドライブ 1 1 1 との間において、共通鍵が改ざんされているとし、処理を終了する。

5 以上のようにして、ドライブ 1 1 1 と A V ボード 1 1 2 との間で、相互認証が行われ、共通鍵が共有されている状態において、これ以降の処理が実行される。

なお、説明は省略するが、さらに、ドライブ 1 1 1 の相互認証部 1 2 1 が、A V ボード 1 1 2 から取得した共通鍵をドライブ 1 1 1 の公開鍵で暗号化したもの、それに対するドライブ 1 1 1 による署名、およびドライブ電子証明書を、A V ボード 1 1 2 に送信し、A V ボード 1 1 2 に認証させるようにしてもよい。

10 次に、図 1 5 のフローチャートを参照して、記録再生装置 1 0 1 の A V ボード 1 1 2 の記録要求処理について説明する。

ステップ S 1 0 1 において、A V コンテンツ処理部 1 3 3 は、コンテンツが入力されるまで待機している。A V コンテンツ処理部 1 3 3 は、アンテナなどにより構成される入力部 1 3 4 を介して放送信号（コンテンツに対応する信号）を受  
15 信すると、ステップ S 1 0 1 において、コンテンツが入力されたと判断し、ステップ S 1 0 2 において、入力されたコンテンツが暗号化またはスクランブルされているか否かに基づいて、入力されたコンテンツが保護すべきコンテンツであるか否かを判断する。

ステップ S 1 0 2 において、A V コンテンツ処理部 1 3 3 は、そのコンテンツ  
20 が保護すべきコンテンツであると判断した場合、暗号化またはスクランブルされているコンテンツを、予め記憶されている鍵（放送信号を送信する機器と共有している鍵）で復号し、ステップ S 1 0 3 において、A V コンテンツ処理部 1 3 3 は、コンテンツ保護部 1 3 2 にブロック鍵生成処理を実行させる。このブロック鍵生成処理を、図 1 6 のフローチャートを参照して説明する。なお、図 1 6 の A  
25 V ボード 1 1 2 におけるブロック鍵生成処理に対応するドライブ 1 1 1 のドライブ情報取得処理も、図 1 7 のフローチャートを参照して、合わせて説明する。

ステップ S 1 2 1 において、R K B 処理部 2 5 2 は、光ディスク 1 4 1 のディ

スク情報（例えば、ディスク I DおよびR K B）の読み出しの要求を、ドライブ 1 1 1に出力する。具体的には、R K B処理部 2 5 2は、光ディスク 1 4 1のディスク I DおよびR K Bの読み出しの要求を、相互認証部 1 3 1に出力する。相互認証部 1 3 1は、ディスク I DおよびR K Bの読み出しの要求を、バス 1 1 3を介して、ドライブ 1 1 1の相互認証部 1 2 1に出力する。

ステップ S 1 4 1において、ドライブ 1 1 1の相互認証部 1 2 1は、バス 1 1 3を介して、A Vボード 1 1 2からの光ディスク 1 4 1のディスク I DおよびR K Bの読み出しの要求を受信する。

ステップ S 1 4 2において、入出力制御部 1 2 2は、相互認証部 1 2 1からの情報に基づいて、このディスク I DおよびR K Bの読み出しの要求をするA Vボード 1 1 2が、ドライブ 1 1 1において相互認証されているか否かを判断する。ステップ S 1 4 2において、A Vボード 1 1 2が、ドライブ 1 1 1において相互認証されていないと判断された場合、ドライブ 1 1 1のディスク情報再生処理は終了する。これにより、不正な装置からの要求は拒絶される。

15 上述したように、A Vボード 1 1 2は、ドライブ 1 1 1において相互認証されているので、ステップ S 1 4 2において、A Vボード 1 1 2が、ドライブ 1 1 1において相互認証されていると判断される。この場合、ステップ S 1 4 3において、記録再生処理部 1 2 3は、光ディスク 1 4 1に記録されているディスク I DおよびR K Bを再生し、相互認証部 1 2 1に供給する。

20 ステップ S 1 4 4において、相互認証部 1 2 1は、記録再生処理部 1 2 3により供給されたディスク I DおよびR K Bを、A Vボード 1 1 2との共通鍵を用いて暗号化し、バス 1 1 3を介して、A Vボード 1 1 2に出力する。

ステップ S 1 2 2において、A Vボード 1 1 2の相互認証部 1 3 1は、バス 1 1 3を介して、暗号化されているディスク I DおよびR K Bを受信し、ドライブ 1 1 1との共通鍵を用いて復号し、R K B処理部 2 5 1に供給する。

ステップ S 1 2 3において、R K B処理部 2 5 1は、供給されたR K Bと内蔵するメモリに予め記憶されているデバイス I Dおよびデバイスキーを作用させて、

ディスク鍵を取得する。具体的には、RKB処理部251は、供給されたRKBと、自身がメモリに記憶しているデバイスID（例えば、図10のデバイス0）、デバイスキー（例えば、図10のデバイス0におけるリーフキーK0000）、およびノードキー（例えば、図10のデバイス0におけるK000, K00, K0, KR）を用いて、プレ記録世代情報 Generation #n（例えば、図12におけるt）時点でのノード00の鍵K(t)00を計算する。そして、RKB処理部251は、供給されたRKBの中から、ディスク鍵K(t)mediaを、鍵K(t)00で暗号化した暗号文Enc(K(t)00, K(t)media)を取得し、これを復号して、ディスク鍵K(t)mediaを取得する。

- 10     ステップS124において、鍵生成部253は、相互認証部131より供給されたディスクID、ステップS123において取得されたディスク鍵、および、コンテンツ保護部132の記録情報などを作用させて、ブロック鍵を生成し、暗号化部254に内蔵されるメモリなどに記憶する。

- 15     以上のようにしてブロック鍵が生成されるので、図15のステップS104において、暗号化部254は、AVコンテンツ処理部133より供給されたコンテンツを、ステップS124において生成されたブロック鍵で暗号化し、相互認証部131に出力する。

- 20     相互認証部131は、ステップS105において、ステップS104においてブロック鍵で暗号化されたコンテンツを、さらに、ドライブ111との共通鍵を用いて、暗号化し、ステップS106において、バス113を介してドライブ111に出力する。

- 25     一方、ステップS102において、AVコンテンツ処理部133より入力されたコンテンツが保護不要のコンテンツであると判断された場合、そのコンテンツは、暗号化部254において暗号化する（光ディスク141上で保護する）必要がなく、相互認証部131においても暗号化する（バス113上で保護する）必要がないため、ステップS103乃至S105の処理は、スキップされる。すなわち、暗号化部254は、そのコンテンツを暗号化させずに（生データのまま



で)、相互認証部 1 3 1 に出力する。ステップ S 1 0 6 において、相互認証部 1 3 1 は、暗号化されていないコンテンツを、バス 1 1 3 を介して、ドライブ 1 1 1 に出力する。

5 以上のようにして、A V ボード 1 1 2 からは、保護すべきコンテンツは、R K B およびディスク I D を作用させたブロック鍵で暗号化される。さらに、保護すべきコンテンツは、ドライブ 1 1 1 との共通鍵で一時的に暗号化され、バス 1 1 3 に出力される。また、保護不要のコンテンツは、生データのまま、バス 1 1 3 に出力される。これに対応して実行されるドライブ 1 1 1 の記録処理を、図 1 8 のフローチャートを参照して説明する。

10 ステップ S 1 6 1 において、ドライブ 1 1 1 の相互認証部 1 2 1 は、バス 1 1 3 を介して、A V ボード 1 1 2 よりコンテンツを受信する。

ステップ S 1 6 2 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 からの情報に基づいて、コンテンツを入力してきた装置が、ドライブ 1 1 1 において相互認証されているか否かを判断する。ステップ S 1 6 2 において、A V ボード 1 1 2 が、ドライブ 1 1 1 において相互認証されていると判断された場合、ステップ S 1 6 3 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドであるかを判断する。

20 ステップ S 1 6 3 において、このコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドであると判断された場合、ステップ S 1 6 4 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 を制御し、受信したコンテンツを、A V ボード 1 1 2 との共通鍵で復号させる。したがって、いま、このコンテンツは、ディスク I D および R K B を作用させたブロック鍵にのみ暗号化された状態となる。

入出力制御部 1 2 2 は、記録再生処理部 1 2 3 を制御し、ステップ S 1 6 5 において、このコンテンツに対応するユーザコントロールデータの U C ( 0 , S )

に、バス 1 1 3 上で保護すべきコンテンツであるという保護情報「0」を生成、格納させ、ステップ S 1 6 8 において、ブロック鍵で暗号化された状態のコンテンツとともに、光ディスク 1 4 1 に記録させる。

一方、例えば、相互認証部を有しない HDD 1 1 4 に記憶されているコンテンツが5 入力される。この場合、ステップ S 1 6 1 において、HDD 1 1 4 からコンテンツが、バス 1 1 3 を介して、相互認証部 1 2 1 に受信される。HDD 1 1 4 は、相互認証部を有しないので、ステップ S 1 6 2 において、コンテンツを入力してきた装置が、ドライブ 1 1 1 において相互認証されていないと判断され、処理は、ステップ S 1 6 6 に進む。ステップ S 1 6 6 において、入出力制御部 1 2 10 2 は、相互認証部 1 2 1 に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドであるか否かを判断する。

ステップ S 1 6 3 において、または、ステップ S 1 6 6 において、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護不要のコンテンツの記録コマンドであると判断された場合、ステップ S 1 6 7 において、入出力制御部 1 2 2 15 は、記録再生処理部 1 2 3 を制御し、コンテンツに対応するユーザコントロールデータの UC (0, S) に、バス 1 1 3 上で保護不要のコンテンツであるという保護情報「1」を生成（格納）させ、生成された保護情報を、ステップ S 1 6 8 において、暗号化されていないコンテンツとともに、光ディスク 1 4 1 に記録さ20 せる。

また、ステップ S 1 6 6 において、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ 1 1 1 の記録処理は、強制的に終了される。したがって、ドライブ 1 1 1 においては、相互認証されない HDD 1 1 4 からのコンテンツは、25 バス 1 1 3 上で保護すべきコンテンツとしては記録されない。

以上のように、相互認証されている AV ボード 1 1 2 からの保護すべきコンテンツは、バス 1 1 3 上で保護すべきコンテンツであるという保護情報「0」とと

もに光ディスク 1 4 1 に記録される。この場合、保護すべきコンテンツは、ディスク I D および R K B を作用させたブロック鍵により暗号化されている。また、相互認証されている A V ボード 1 1 2 からの保護不要のコンテンツ、または、相互認証されていない H D D 1 1 4 からの保護不要のコンテンツは、バス 1 1 3 上で保護不要のコンテンツであるという保護情報「1」とともに光ディスク 1 4 1 に記憶される。この場合、保護不要のコンテンツは、暗号化されていない。

以上のようにして格納された保護情報は、次に説明するドライブ 1 1 1 のコンテンツ再生処理により再生され、利用される。図 1 9 のフローチャートを参照して、ドライブ 1 1 1 のコンテンツ再生処理について説明する。

- 10 ユーザは、光ディスク 1 4 1 に記録されている保護すべきコンテンツを、A V ボード 1 1 2 の出力部 1 3 5 から出力させるために、図示せぬ操作入力部などを介して、A V ボード 1 1 2 に、コンテンツの再生コマンドを入力する。A V ボード 1 1 2 の相互認証部 1 3 1 は、バス 1 1 3 を介して、ドライブ 1 1 1 に再生コマンドを送信してくるので、ステップ S 1 9 1 において、相互認証部 1 2 1 は、
- 15 A V ボード 1 1 2 からの再生コマンドを入力する。

- ステップ S 1 9 2 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 からの情報に基づいて、コンテンツを出力する機器（いまの場合、A V ボード 1 1 2）が、ドライブ 1 1 1 において相互認証されているか否かを判断する。ステップ S 1 9 2 において、A V ボード 1 1 2 が相互認証されていると判断された場合、
- 20 テップ S 1 9 3 において、入出力制御部 1 2 2 は、A V ボード 1 1 2 からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かを判断する。

- ステップ S 1 9 3 において、A V ボード 1 1 2 からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、ステップ S 1 9 4 において、記録再生処理部 1 2 3 は、光ディスク 1 4 1 から指示されたコンテンツを
- 25 再生する。

図 5 を参照して上述したように、光ディスク 1 4 1 に記録された保護情報（ユーザコントロールデータ）は、コンテンツを再生する場合、そのコンテンツより

も先に再生されるので、ステップ S 1 9 5 において、入出力制御部 1 2 2 は、そのコンテンツに対応するユーザコントロールデータの UC ( 0 , S ) が「 0 」であるか否かを判断し、コンテンツに対応する UC ( 0 , S ) が「 0 」であると判断された場合、このコンテンツはバス 1 1 3 上で保護すべきコンテンツであるこ

5      となるので、ステップ S 1 9 6 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 を制御し、AV ボード 1 1 2 との共通鍵を用いて、再生されたコンテンツを暗号化させ、バス 1 1 3 を介して AV ボード 1 1 2 に出力させる。したがって、バス 1 1 3 上における不正なデータの取得（ハッキング）が防止される。

10      ステップ S 1 9 5 において、コンテンツに対応する UC ( 0 , S ) が「 0 」ではないと判断された場合（コンテンツに対応する UC ( 0 , S ) が「 1 」であると判断された場合）、このコンテンツは、バス 1 1 3 上で保護不要のコンテンツであるため、AV ボード 1 1 2 からの保護すべきコンテンツの再生コマンドと矛盾するため、ドライブ 1 1 1 の再生処理は終了する。すなわち、ドライブ 1 1 1 は、バス 1 1 3 上へのデータの出力を行わないように制御される。

15      一方、例えば、ユーザは、光ディスク 1 4 1 に記録されている保護不要のコンテンツを、HDD 1 1 4 に保存（記録）させるために、図示せぬ操作入力部などを介して、HDD 1 1 4 に、コンテンツの再生コマンドを入力する。HDD 1 1 4 は、バス 1 1 3 を介して、ドライブ 1 1 1 に再生コマンドを送信してくるので、ステップ S 1 9 1 において、相互認証部 1 2 1 は、HDD 1 1 4 からの再生コマ  
20      ンドを入力する。

25      ステップ S 1 9 2 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 からの情報に基づいて、コンテンツを出力する機器（いまの場合、HDD 1 1 4）が、相互認証されていないと判断する。このとき、ステップ S 1 9 7 において、入出力制御部 1 2 2 は、HDD 1 1 4 からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かを判断する。

30      ステップ S 1 9 3 において、または、ステップ S 1 9 7 において、コンテンツを出力する機器からの再生コマンドが、保護不要のコンテンツの再生コマンドで

あると判断された場合、ステップS 1 9 8において、記録再生処理部1 2 3は、光ディスク1 4 1から指示されたコンテンツを再生する。ステップS 1 9 9において、入出力制御部1 2 2は、そのコンテンツに対応するユーザコントロールデータのUC (0, S) が「1」であるか否かを判断する。コンテンツに対応する

5 UC (0, S) が「1」であると判断された場合、このコンテンツがバス1 1 3上で保護不要のコンテンツであることになるので、ステップS 2 0 0において、入出力制御部1 2 2は、相互認証部1 2 1を制御し、再生されたコンテンツをそのまま（生データのまま）、バス1 1 3を介してコンテンツを出力する機器（いまの場合、AVボード1 1 2またはHDD 1 1 4）に出力させる。

10 また、ステップS 1 9 7において、HDD 1 1 4からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップS 1 9 9において、コンテンツに対応するUC (0, S) が「1」ではないと判断された場合（コンテンツに対応するUC (0, S) が「0」であると判断された場合）、相互認証されていないHDD 1 1 4へは、保護すべきコンテンツの出力は

15 できないので、エラーとなり、ドライブ1 1 1の出力処理は、強制的に終了される。すなわち、ドライブ1 1 1においては、HDD 1 1 4から保護すべきコンテンツの再生コマンドは拒否される。また、保護不要のコンテンツの再生コマンドであったとしても、実際にバス1 1 3上において、保護すべきコンテンツであった場合は、出力されない。

20 以上のようにして、相互認証されているAVボード1 1 2への再生コマンドに対して、バス1 1 3上で保護すべきコンテンツは、共通鍵で暗号化され、バス1 1 3を介して、AVボード1 1 2に出力され、バス1 1 3上で保護不要のコンテンツは、そのまま（暗号化させずに）、バス1 1 3を介して、AVボード1 1 2に出力される。そして、後述する図2 0のステップS 2 0 1において、AVボ

25 ド1 1 2の相互認証部1 3 1により受信される。

一方、相互認証されていないHDD 1 1 4への再生コマンドに対しては、バス1 1 3上で保護すべきコンテンツは、出力されないが、バス1 1 3上で保護不要

のコンテンツは、そのまま（暗号化させずに）、バス 1 1 3 を介して、HDD 1 1 4 に出力される。これにより、HDD 1 1 4 において、保護不要のコンテンツが記憶できるので、ストレージ運用が可能になる。

また、保護されるべきコンテンツは、ディスク ID および RKB を作用させた  
5 ブロック鍵、およびコンテンツを送受信する装置間（いまの場合、ドライブ 1 1 1 および AV ボード 1 1 2）における相互認証されている共通鍵の両方で暗号化されているため、汎用的なバス 1 1 3 を介しても、不当なコピーを抑制することができる。

なお、既存の記録再生装置において光ディスクに記録された保護すべきコンテ  
10 ンツに対応するユーザコントロールデータ 2 0 2（1 8 バイト）の先頭バイト UC（0，S）の最下位ビットには、もともと「0」が格納されている。したがって、既存のデータフォーマットにより記録した保護すべきコンテンツに対しても、上述した保護すべきコンテンツの再生処理が実行される（相互認証されている機器に対しては、共通鍵で暗号されて出力され、相互認証されていない機器に対し  
15 ては、出力が禁止される）ので、汎用的なバス 1 1 3 を介しても、不当なコピーを抑制することができる。すなわち、既存のものと互換性が保たれる。

以上のようなドライブ 1 1 1 のコンテンツ再生処理に対応する AV ボード 1 1 2 の再生処理を、図 2 0 のフローチャートを参照して説明する。

ドライブ 1 1 1 は、AV ボード 1 1 2 からの保護すべきコンテンツの再生コマ  
20 ンドを受信し、光ディスク 1 4 1 よりコンテンツを再生し、バス 1 1 3 を介して出力してくるので、AV ボード 1 1 2 の相互認証部 1 3 1 は、ステップ S 2 0 1 において、そのコンテンツを受信し、ステップ S 2 0 2 において、受信したコンテンツが、ドライブ 1 1 1 の相互認証部 1 2 1 により暗号化されているか（保護すべきコンテンツであるか）否かを判断する。

25 ステップ S 2 0 2 において、そのコンテンツが、共通鍵を用いて暗号化されており、保護すべきコンテンツであると判断された場合、ステップ S 2 0 3 において、相互認証部 1 3 1 は、ドライブ 1 1 1 との共通鍵を用いて、受信されたコン

テンツを復号し、コンテンツ保護部 1 3 2 に出力する。すなわち、いま、このコンテンツは、ディスク I D および R K B を作用させたブロック鍵のみにより暗号化されている状態である。

5      ステップ S 2 0 4 において、コンテンツ保護部 1 3 2 は、ブロック鍵の生成処理を実行する。なお、このブロック鍵の生成処理は、図 1 6 を参照して説明したブロック鍵生成処理と同様であるので、その説明は繰り返しになるので、省略するが、ステップ S 2 0 4 において、光ディスク 1 4 1 の R K B を作用させたディスク鍵が取得され、取得されたディスク鍵および光ディスク 1 4 1 のディスク I D が生成されるので、ステップ S 2 0 5 において、暗号化部 2 5 4 は、相互認証  
10   部 1 3 1 からのコンテンツを、ブロック鍵を用いて復号し、A V コンテンツ処理部 1 3 3 に供給する。

一方、ステップ S 2 0 2 において、受信したコンテンツが、暗号化されておらず、保護不要のコンテンツであると判断された場合、このコンテンツは復号する必要はない。したがって、相互認証部 1 3 1 およびコンテンツ保護部 1 3 2 を素  
15   通りするため、ステップ S 2 0 3 乃至 S 2 0 5 の処理はスキップされる。

ステップ S 2 0 6 において、A V コンテンツ処理部 1 3 3 は、コンテンツ保護部 1 3 2 から供給されたコンテンツを、例えば、MPEG (Moving Picture Experts Group) 方式でデコードし、再生する。ステップ S 2 0 7 において、出力部  
1 3 5 は、再生されたコンテンツを出力する。

20   以上のようにして、ドライブ 1 1 1 と相互認証されている A V ボード 1 1 2 においては、光ディスク 1 4 1 に記録されている保護すべきコンテンツおよび保護不要のコンテンツの両方を出力することができる。

なお、上記説明においては、A V ボード 1 1 2 は、記録時および再生時に、保護すべきコンテンツであると判断してからブロック鍵を生成するように説明したが、このブロック鍵の生成処理は、光ディスク 1 4 1 が装着されるごとに A V  
25   ボード 1 1 2 の保護コンテンツ部 1 3 2 において実行されるようにしてもよい。

図 2 1 は、本発明の記録再生装置の他の構成例を示している。なお、図 2 1 の

記録再生装置 301 の基本的な構成は、図 4 の記録再生装置 101 と同様であるが、図 21 の記録再生装置 301 においては、図 4 の記録再生装置 101 におけるドライブ 111 の相互認証部 121 が除かれている。

したがって、図 21 の記録再生装置 301 においては、AV ボード 112 は、  
5 バス 113 上に接続されていても、ドライブ 111 が、相互認証機能を有しないため、AV ボード 112 において相互認証されず（共通鍵が共有されず）、AV ボード 112 からのコンテンツの再生要求処理は実行されないが、相互認証機能を有しない HDD 114 との保護不要のコンテンツの送受信処理が実行される。

この記録再生装置 301 のドライブ 111 の記録処理を、図 22 のフローチャート  
10 ートを参照して説明する。なお、図 22 のステップ S211 乃至 S214 は、図 18 のステップ S161 およびステップ S166 乃至 S168 と同様の処理であり、その詳細な説明は繰り返しになるので省略する。

ステップ S211 において、HDD 114 からの保護不要のコンテンツが、バス 113  
15 を介して記録再生処理部 123 に受信される。ステップ S212 において、入出力制御部 122 により、記録再生処理部 123 に入力されたコンテンツが共通鍵で暗号化されていないので、いまの記録コマンドが、バス 113 上で保護すべきコンテンツの記録コマンドではないと判断される。ステップ S213 において、記録再生処理部 123 により、コンテンツに対応するユーザコントロールデータの UC (0, S) に、バス 113 上で保護不要のコンテンツであるとい  
20 う保護情報「1」が生成、格納され、ステップ S214 において、記録再生処理部 123 により、この HDD 114 からの保護不要のコンテンツが光ディスク 141 に記録される。

また、ステップ S212 において、共通鍵で暗号化されているコンテンツが入力され、いまの記録コマンドが、保護すべきコンテンツの記録コマンドであると  
25 判断された場合、エラーとなり、ドライブ 111 の記録処理は、強制的に終了される。

以上のようにして、相互認証機能を有さない HDD 114 からのバス 113 上



で保護不要の保護情報ともに、コンテンツが光ディスク 1 4 1 に記録される。

次に、この記録再生装置 3 0 1 のドライブ 1 1 1 の再生処理を、図 2 3 のフローチャートを参照して説明する。なお、図 2 3 のステップ S 2 2 1 乃至 S 2 2 5 の処理は、図 1 9 のステップ S 1 9 1 およびステップ S 1 9 7 乃至 S 2 0 0 の処理と同様の処理であり、その詳細な説明は繰り返しになるので省略する。

したがって、例えば、ユーザは、光ディスク 1 4 1 に記録されている保護不要のコンテンツを、HDD 1 1 4 に保存（記録）させるために、入力部を介して、HDD 1 1 4 へのコンテンツの再生コマンドを入力する。HDD 1 1 4 は、バス 1 1 3 を介して、ドライブ 1 1 1 に再生コマンドを送信してくる。ステップ S 2 2 1 において、HDD 1 1 4 からの再生コマンドが入力される。ステップ S 2 2 2 において、入出力制御部 1 2 2 により、HDD 1 1 4 からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップ S 2 2 3 において、記録再生処理部 1 2 3 により、指示されたコンテンツが光ディスク 1 4 1 から再生される。

ステップ S 2 2 4 において、入出力制御部 1 2 2 により、そのコンテンツに対応するユーザコントロールデータの UC ( 0 , S ) が「1」とであると判断された場合、バス 1 1 3 上で保護不要のコンテンツであるとされる。ステップ S 2 2 5 において、記録再生処理部 1 2 3 により再生されたコンテンツがそのまま（生データのまま）、バス 1 1 3 を介して HDD 1 1 4 に出力される。

一方、ステップ S 2 2 2 において、HDD 1 1 4 からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップ S 2 2 4 において、コンテンツに対応する UC ( 0 , S ) が「1」ではないと判断された場合、相互認証されていない HDD 1 1 4 へは、バス 1 1 3 上において保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ 1 1 1 の記録処理は、強制的に終了される。

以上のようにして、HDD 1 1 4 への再生コマンドに対して、保護情報「1」が再生された場合、再生された、バス 1 1 3 上での保護不要のコンテンツは、そ

のまま（暗号化させずに）、バス 1 1 3 を介して、HDD 1 4 に出力される。したがって、保護不要のコンテンツは、共通鍵により暗号化もされていないので、HDD 1 4 に供給され、記憶されるようにできる。これにより、HDD 1 4 において、ストレージ運用が可能になる。

5 図 2 4 は、本発明を適用したさらに他の記録再生装置の構成例を示している。図 2 4 の記録再生装置 4 0 1 は、図 4 の記録再生装置 1 0 1 と基本的に同様な構成とされるが、図 2 4 の A V ボード 1 1 2 においては、図 4 の A V ボード 1 1 2 のコンテンツ保護部 1 3 2 が除かれており、代わりに、ドライブ 1 1 1 にコンテンツ保護部 4 1 1 が配置されている構成になっている。

10 したがって、図 2 4 の A V ボード 1 1 2 においては、A V コンテンツ処理部 1 3 3 から供給されるコンテンツは、相互認証部 1 3 1 に出力される。相互認証部 1 3 1 より出力されるコンテンツは、A V コンテンツ処理部 1 3 3 に供給される。

また、図 2 4 のドライブ 1 1 1 においては、相互認証部 1 2 1 に入力されたコンテンツは、コンテンツ保護部 4 1 1 に供給される。コンテンツ保護部 4 1 1 の基本的な構成は、図 4 のコンテンツ保護部 1 3 2 と同様である。したがって、コンテンツ保護部 4 1 1 は、相互認証部 1 2 1 から供給されたコンテンツを、入出力制御部 1 2 2 の制御のもと、光ディスク 1 4 1 のディスク ID および R K B（ディスク鍵）を作用させたブロック鍵、または、R K B（ディスク鍵）のみを作用させたブロック鍵により暗号化し、記録再生処理部 1 2 3 に出力する。

20 記録再生処理部 1 2 3 は、光ディスク 1 4 1 から再生されたコンテンツを、コンテンツ保護部 4 1 1 に供給する。コンテンツ保護部 4 1 1 は、入出力制御部 1 2 2 の制御のもと、光ディスク 1 4 1 のディスク ID および R K B を作用させたブロック鍵、または、R K B のみを作用させたブロック鍵により復号し、相互認証部 1 2 1 に出力する。

25 図 2 5 は、図 2 4 のコンテンツ保護部 4 1 1 の構成を示している。なお、図 2 4 のコンテンツ保護部 4 1 1 は、図 9 のコンテンツ保護部 1 3 2 と基本的に同様の構成を有している。したがって、例えば、入出力制御部 1 2 2 により、A V ボ

ード1 1 2からの入力されたコンテンツが保護すべきコンテンツである（入力されたコンテンツの記録コマンドが、保護すべきコンテンツの記録コマンドである）と判断された場合、暗号化部2 5 4は、ディスク鍵、ディスクIDおよび記録情報を作用させて生成された、保護すべきコンテンツ用のブロック鍵を用いて、

5 コンテンツを暗号化する。

また、入出力制御部1 2 2によりAVボード1 1 2からの入力されたコンテンツが保護不要のコンテンツである（入力されたコンテンツの記録コマンドが、保護不要のコンテンツの記録コマンドである）と判断された場合、暗号化部2 5 4は、少なくともRKBにより作成されたディスク鍵を作用させて生成された、保護不要のコンテンツ用のブロック鍵を用いて、コンテンツを暗号化する。RKB

10 により作成されたディスク鍵を作用させるのは、不正なドライブを排除するようにするためである。なお、これらの保護すべきコンテンツ用および保護不要のコンテンツ用のブロック鍵は、ドライブ1 1 1に光ディスク1 4 1が新しく装着される毎に、図2 6を参照して後述するブロック鍵生成処理により予め作成され、

15 暗号化部2 5 4に内蔵されるメモリ（図示せず）に記憶されている。

次に、図2 6のフローチャートを参照して、図2 4のコンテンツ保護部4 1 1のブロック鍵生成処理を説明する。

ステップS 2 4 1において、記録再生処理部1 2 3は、ドライブ1 1 1に新しく光ディスク1 4 1が装着されるまで待機しており、ステップS 2 4 1において、

20 光ディスク1 4 1が装着されたと判断した場合、ステップS 2 4 2において、記録再生処理部1 2 3は、光ディスク1 4 1に記録されているディスクIDおよびRKB（ディスク情報）を再生し、コンテンツ保護部4 1 1に供給する。

ステップS 2 4 3において、RKB処理部2 5 2は、供給されたRKBと内蔵するメモリに予め記憶されているデバイスIDおよびデバイスキーを用いて、

25 ディスク鍵を取得する。なお、この処理は、図1 6のステップS 1 2 3の処理と同様であるため、その説明は繰り返しになるので省略する。

ステップS 2 4 4において、鍵生成部2 5 3は、記録再生処理部1 2 3より供

給されたディスクID、ステップS243において生成されたディスク鍵、および、コンテンツ保護部411の記録情報などを作用させて、保護すべきコンテンツ用のブロック鍵を生成し、暗号化部254に内蔵されるメモリなどに記憶する。

5     ステップS245において、鍵生成部253は、少なくとも、ステップS243において生成されたディスク鍵を作用させて、保護不要のコンテンツ用のブロック鍵を生成し、暗号化部254に内蔵されるメモリなどに記憶する。

10    以上のように、図24のコンテンツ保護部411においては、光ディスク141が装着されるたびに、保護すべきコンテンツ用および保護不要のコンテンツ用の2種類のブロック鍵が生成され、記憶される。なお、上記説明においては、ブロック鍵を生成したが、ブロック鍵を生成するためのディスクID、ディスク鍵などを記憶しておき、暗号化する際に、そのコンテンツの保護状態に応じて、ブロック鍵を生成するようにしてもよい。

15    次に、図27のフローチャートを参照して、図24のAVボード112の記録要求処理を説明する。なお、図27の記録要求処理は、図15の記録要求処理のステップS103およびS104が除かれている点を除き、図15の記録要求処理を同様の処理である。

したがって、ドライブ111においては、相互認証され、共通鍵が、AVボード112と共有されている状態において、それ以降の処理が実行される。

20    ステップS261において、AVコンテンツ処理部133によりコンテンツが入力される。ステップS262において、AVコンテンツ処理部133により保護すべきコンテンツであると判断された場合、ステップS263において、そのコンテンツが、相互認証部131により、ドライブ111との共通鍵を用いて暗号化される。ステップS264において、暗号化されたコンテンツがドライブ111に出力される。ステップS262において、保護不要のコンテンツであると判断されると、暗号化せず（ステップS263の処理はスキップされ）、ステップS264において、ドライブ111に出力される。

以上のようにして、AVボード112からは、保護すべきコンテンツがドライ

5 プ 1 1 1 との共通鍵を用いて暗号化され、出力される。また、保護不要のコンテンツは、そのまま出力される。これに対応して実行される図 2 4 のドライブ 1 1 1 の記録処理を、図 2 8 のフローチャートを参照して説明する。なお、図 2 8 のステップ S 3 0 1 乃至 S 3 0 4、ステップ S 3 0 6 および S 3 0 7、並びにステップ S 3 0 9 および S 3 1 0 は、図 1 8 のステップ S 1 6 1 乃至 S 1 6 8 と同様の処理であるため、その詳細な説明は省略する。

ステップ S 3 0 1 において、ドライブ 1 1 1 の相互認証部 1 2 1 は、バス 1 1 3 を介して、A V ボード 1 1 2 よりコンテンツを受信する。

10 ステップ S 3 0 2 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 からの情報に基づいて、このコンテンツを入力してきた A V ボード 1 1 2 が、ドライブ 1 1 1 において相互認証されているか否かを判断し、A V ボード 1 1 2 が、ドライブ 1 1 1 において相互認証されていると判断された場合、ステップ S 3 0 3 において、入出力制御部 1 2 2 は、相互認証部 1 2 1 に入力されたコンテンツが共通鍵により暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドであるかを判断する。

15 ステップ S 3 0 3 において、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドであると判断された場合、ステップ S 3 0 4 において入出力制御部 1 2 2 は、相互認証部 1 2 1 を制御し、受信したコンテンツを、A V ボード 1 1 2 との共通鍵で復号させ、そのコンテンツをコンテンツ保護部 4 1 1 に供給させる。

20 ステップ S 3 0 5 において、暗号化部 2 5 4 は、供給されたコンテンツを、保護すべきコンテンツ用のブロック鍵を用いて暗号化する。この保護すべきコンテンツ用のブロック鍵は、図 2 6 を参照して上述したように、暗号化部 2 5 4 のメモリ内に予め記憶されている。そして、入出力制御部 1 2 2 は、記録再生処理部 1 2 3 を制御し、ステップ S 3 0 6 において、このコンテンツに対応するユーザコントロールデータの U C ( 0 , S ) に、バス 1 1 3 上で保護すべきコンテンツ

であるという保護情報「0」を生成、格納させ、ステップS310において、保護すべきコンテンツ用のブロック鍵を用いて暗号化されたコンテンツとともに、光ディスク141に記録させる。

一方、例えば、相互認証部を有しないHDD114に記憶されているコンテンツが5 入力される。このとき、ステップS301において、HDD114からのコンテンツが、バス113を介して相互認証部121に受信される。ステップS302において、コンテンツを入力してきた装置がドライブ111において相互認証されていないと判断される。ステップS307において、入出力制御部122により、相互認証部121に入力されたコンテンツが共通鍵で暗号化されている10 か否かに基づいて、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであるか否かが判断される。

ステップS303において、または、ステップS307において、入力されたコンテンツの記録コマンドが、バス113上で保護不要のコンテンツの記録コマンドであると判断された場合、ステップS308において、暗号化部254は、15 相互認証部121より供給されたコンテンツを、保護不要のコンテンツ用のブロック鍵を用いて暗号化する。この保護不要のコンテンツ用のブロック鍵は、図26を参照して上述したように、暗号化部254のメモリ内に予め記憶されている。

ステップS309において、入出力制御部122は、記録再生処理部123を制御し、コンテンツに対応するユーザコントロールデータのUC(0, S)に、20 バス113上で保護不要のコンテンツであるという保護情報「1」を生成、格納させ、ステップS310において、生成された保護情報を、コンテンツとともに、光ディスク141に記録させる。

また、ステップS307において、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであると判断された場合、25 エラーとなり、ドライブ111の記録処理は、強制的に終了される。

以上のようにして、相互認証されているAVボード112からの保護すべきコンテンツは、ディスクIDおよびRKBを作用させたブロック鍵で暗号化され、

バス 1 1 3 上で保護すべきコンテンツであるという保護情報「0」とともに光ディスク 1 4 1 に記録される。また、相互認証されている A V ボード 1 1 2 からの保護不要のコンテンツ、または、相互認証されていない H D D 1 1 4 からの保護不要のコンテンツは、R K B のみを作用させたブロック鍵で暗号化され、バス 1 1 3 上で保護不要のコンテンツであるという保護情報「1」とともに光ディスク 1 4 1 に記録される。さらに、相互認証されていない H D D 1 1 4 からの保護すべきコンテンツは、光ディスク 1 4 1 には、記録されない。

次に、図 2 9 のフローチャートを参照して、図 2 4 のドライブ 1 1 1 のコンテンツ再生処理について説明する。なお、図 2 9 のステップ S 3 2 1 乃至 S 3 2 5、並びにステップ S 3 2 7 乃至 S 3 3 0 は、図 1 9 のステップ S 1 9 1 乃至 S 2 0 0 と同様の処理であるため、その詳細な説明は省略する。

ユーザは、光ディスク 1 4 1 に記録されている保護すべきコンテンツを、A V ボード 1 1 2 の出力部 1 3 5 から出力させるために、操作入力部を介して、A V ボード 1 1 2 に、コンテンツの再生コマンドを入力する。A V ボード 1 1 2 の相互認証部 1 3 1 は、バス 1 1 3 を介して、ドライブ 1 1 1 に再生コマンドを送信してくる。ステップ S 3 2 1 において、相互認証部 1 2 1 は、A V ボード 1 1 2 からの再生コマンドを入力する。ステップ S 3 2 2 において、相互認証部 1 2 1 からの情報に基づいて、コンテンツを出力する A V ボード 1 1 2 が、ドライブ 1 1 1 において相互認証されていると判断された場合、ステップ S 3 2 3 において、入出力制御部 1 2 2 により、A V ボード 1 1 2 からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かが判断される。

ステップ S 3 2 3 において、A V ボード 1 1 2 からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、ステップ S 3 2 4 において、記録再生処理部 1 2 3 により、光ディスク 1 4 1 から指示されたコンテンツが再生される。ステップ S 3 2 5 において、入出力制御部 1 2 2 により、そのコンテンツに対応するユーザコントロールデータの U C ( 0 , S ) が「0」であると判断された場合、再生されたコンテンツがバス 1 1 3 上で保護すべきコンテ

ンツであるものとされる。ステップS 3 2 6において、暗号化部 2 5 4 は、内蔵するメモリに記憶された保護すべきコンテンツ用のブロック鍵を用いて、再生されたコンテンツを復号する。ステップS 3 2 7において、相互認証部 1 2 1 は、暗号化部 2 5 4 より供給されたコンテンツを、AVボード 1 1 2 との共通鍵を用いて暗号化し、バス 1 1 3 を介してAVボード 1 1 2 に出力する。

一方、例えば、ユーザは、光ディスク 1 4 1 に記録されている保護不要のコンテンツを、HDD 1 1 4 に保存（記録）させるために、操作入力部を介して、HDD 1 1 4 にコンテンツの再生コマンドを入力する。HDD 1 1 4 は、バス 1 1 3 を介して、ドライブ 1 1 1 に再生コマンドを送信してくるので、ステップS 3 2 1 において、相互認証部 1 2 1 は、HDD 1 1 4 からの再生コマンドを入力する。ステップS 3 2 2 において、相互認証部 1 2 1 からの情報に基づいて、コンテンツを出力するHDD 1 1 4 が、相互認証されていないと判断され、ステップS 3 2 8 において、HDD 1 1 4 からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かが判断される。

ステップS 3 2 3 において、または、ステップS 3 2 8 において、HDD 1 1 4 からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップS 3 2 9 において、記録再生処理部 1 2 3 により指示されたコンテンツが光ディスク 1 4 1 から再生され、ステップS 3 3 0 において、入出力制御部 1 2 2 は、そのコンテンツに対応するユーザコントロールデータのUC (0, S) が「1」であるか否かを判断する。ステップS 3 3 0 において、入出力制御部 1 2 2 によりそのコンテンツに対応するユーザコントロールデータのUC (0, S) が「1」であると判断された場合、再生されたコンテンツがバス 1 1 3 上で保護不要のコンテンツであるとする。ステップS 3 3 1 において暗号化部 2 5 4 は、内蔵するメモリに記憶された保護不要のコンテンツ用のブロック鍵を用いて、復号し、コンテンツをそのまま（生データのまま）、相互認証部 1 2 1 およびバス 1 1 3 を介して、AVボード 1 1 2 またはHDD 1 1 4 に出力する。

また、ステップS 3 2 5 において、コンテンツに対応するUC (0, S) が



「0」ではないと判断された場合、ステップS 3 2 8において、HDD 1 1 4からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップS 3 3 0において、コンテンツに対応するUC (0, S) が「1」ではないと判断された場合、エラーとなり、ドライブ1 1 1の記録  
5 処理は、強制的に終了される。

以上のようにして、相互認証されているAVボード1 1 2からの再生コマンドに対して、バス1 1 3上で保護すべきコンテンツは、共通鍵で暗号化され、バス1 1 3を介して、AVボード1 1 2に出力され、バス1 1 3上で保護不要のコンテンツは、そのまま（暗号化させずに）、バス1 1 3を介して、AVボード1 1  
10 2に出力される。そして、後述する図30のステップS 3 6 1において、AVボード1 1 2の相互認証部1 3 1により受信される。

この図29のドライブ1 1 1のコンテンツ再生処理に対応するAVボード1 1 2の再生処理を、図30のフローチャートを参照して説明する。なお、図30の再生処理は、図20の再生処理のステップS 2 0 4およびS 2 0 5を省略した点  
15 を除き、図20の場合と同様である。

ステップS 3 6 1において、相互認証部1 3 1により、ドライブ1 1 1からのコンテンツが受信され、ステップS 3 6 2において、そのコンテンツが、共通鍵を用いて暗号化されており、保護すべきコンテンツであると判断された場合、ステップS 3 6 3において、ドライブ1 1 1との共通鍵を用いて受信されたコンテ  
20 ンツが復号される。

一方、ステップS 3 6 2において、暗号化されておらず、保護不要のコンテンツであると判断された場合、このコンテンツは、暗号化されていないので、復号する必要はない。したがって、相互認証部1 3 1およびコンテンツ保護部1 3 2を素通りするため、ステップS 3 6 3の処理はスキップされる。

25 ステップS 3 6 4において、AVコンテンツ処理部1 3 3は、コンテンツ保護部1 3 2から供給されたコンテンツを、例えば、MPEG方式でデコードし、再生する。ステップS 3 6 5において、出力部1 3 5は、再生されたコンテンツを出

力する。

以上のようにして、ドライブ 1 1 1 と相互認証されている A V ボード 1 1 2 においては、光ディスク 1 4 1 に記録されているバス 1 1 3 上で保護すべきコンテンツ、および、バス 1 1 3 上で保護不要のコンテンツの両方を出力することができる。

図 3 1 は、本発明の記録再生装置の他の構成例を示している。なお、図 3 1 の記録再生装置 5 0 1 の基本的な構成は、図 2 4 の記録再生装置 4 0 1 と同様であるが、図 3 1 の記録再生装置 5 0 1 においては、図 2 4 の記録再生装置 4 0 1 におけるドライブ 1 1 1 の相互認証部 1 2 1 が除かれている。

したがって、図 3 1 の記録再生装置 5 0 1 においては、A V ボード 1 1 2 は、バス 1 1 3 上に接続されていても、ドライブ 1 1 1 が、相互認証機能を有しないため、A V ボード 1 1 2 において相互認証されず（共通鍵が共有されず）、A V ボード 1 1 2 からのコンテンツの再生要求処理は実行されないが、相互認証機能を有しない HDD 1 1 4 との保護不要のコンテンツの送受信処理が実行される。

この記録再生装置 5 0 1 のドライブ 1 1 1 の記録処理を、図 3 2 のフローチャートを参照して説明する。なお、図 3 2 のステップ S 4 0 1 乃至 S 4 0 5 は、図 2 8 のステップ S 3 0 1 およびステップ S 3 0 7 乃至 S 3 1 0 と同様の処理であり、その説明は繰り返しになるので適宜省略する。

したがって、ステップ S 4 0 1 において、HDD 1 1 4 からの保護不要のコンテンツが、バス 1 1 3 を介して記録再生処理部 1 2 3 に受信され、ステップ S 4 0 2 において、入出力制御部 1 2 2 により、相互認証部 1 2 1 に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス 1 1 3 上で保護すべきコンテンツの記録コマンドではないと判断される。ステップ S 4 0 3 において、暗号化部 2 5 4 により、保護不要のコンテンツ用のブロック鍵を用いて、コンテンツが暗号化される。

ステップ S 4 0 4 において、記録再生処理部 1 2 3 により、コンテンツに対応するユーザコントロールデータの UC ( 0 , S ) に、バス 1 1 3 上で保護不要の

コンテンツであるという保護情報「1」が生成、格納され、ステップS 4 0 5において、HDD 1 1 4からの保護不要のコンテンツとともに、光ディスク 1 4 1に記録される。

また、ステップS 4 0 2において、共通鍵で暗号化されているコンテンツが入力され、入力されたコンテンツの記録コマンドが、バス 1 1 3上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ 1 1 1の記録処理は、強制的に終了される。なお、共通鍵ではなく別の方法で暗号化されているコンテンツであれば、バス 1 1 3上で保護不要のコンテンツとして処理させることも可能である。

10 以上のようにして、相互認証機能を有さないHDD 1 1 4からのバス 1 1 3上で保護不要のコンテンツが光ディスク 1 4 1に記録される。

次に、この記録再生装置 5 0 1のドライブ 1 1 1の再生処理を、図 3 3のフローチャートを参照して説明する。なお、図 3 3のステップS 4 2 1乃至S 4 2 5は、図 2 9のステップS 3 2 1およびステップS 3 2 8乃至S 3 3 1と同様の処理であるため、その詳細な説明を省略する。

したがって、例えば、ユーザは、光ディスク 1 4 1に記録されている保護不要のコンテンツを、HDD 1 1 4に保存（記録）させるために、操作入力部を介して、HDD 1 1 4に、保護不要のコンテンツの再生コマンドを入力する。HDD 1 1 4は、バス 1 1 3を介して、ドライブ 1 1 1に再生コマンドを送信してくるので、ステップS 4 2 1において、HDD 1 1 4からの再生コマンドが入力され、ステップS 4 2 2において、HDD 1 1 4からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップS 4 2 3において、記録再生処理部 1 2 3により、光ディスク 1 4 1から指示されたコンテンツが再生される。

25 ステップS 4 2 4において、入出力制御部 1 2 2により、そのコンテンツに対応するユーザコントロールデータのUC (0, S)が「1」とであると判断された場合、再生されたコンテンツがバス 1 1 3上で保護不要のコンテンツであるとさ

れ、ステップS 4 2 5において、暗号化部 2 5 4により、保護不要のコンテンツ用のブロック鍵を用いて、復号され、コンテンツが、そのまま（生データのま）ま）、相互認証部 1 2 1およびバス 1 1 3を介してコンテンツを出力するAVボード 1 1 2またはHDD 1 1 4に出力される。

- 5      一方、ステップS 4 2 2において、HDD 1 1 4からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップS 4 2 4において、コンテンツに対応するUC (0, S) が「1」ではないと判断された場合、相互認証されていないHDD 1 1 4へは、保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ 1 1 1の記録処理は、強制的に終了される。
- 10    れる。

- 以上のようにして、HDD 1 1 4への再生コマンドに対して、保護情報「1」が再生され、再生された保護不要のコンテンツは、そのまま（暗号化させずに）、バス 1 1 3を介して、HDD 1 4に出力される。したがって、バス 1 1 3上で保護不要のコンテンツは、暗号化もされていないので、HDD 1 4に供給され、記憶されるようにできる。
- 15    憶されるようにできる。

- また、相互認証されないHDD 1 4からのコンテンツは、HDD 1 4により保護すべきコンテンツであると示されたとしても、ドライブ 1 1 1においては、保護すべきコンテンツとしては認識されず、保護不要のコンテンツとしてであれば、扱うようにできる。以上のように、コピーフリーのコンテンツのみを扱う相互認証しないストレージ運用が可能になる。
- 20    証しないストレージ運用が可能になる。

    なお、上記説明においては、記録媒体を、光ディスク 1 4 1としたが、記録媒体は、光ディスク 1 4 1だけでなく、光ディスク 1 4 1以外のメモリーカード（登録商標）、その他の記録媒体とすることもできる。

- 上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。この場合、例えば、図 4 の記録再生装置 1 0 1、図 2 1 の記録再生装置 3 0 1、図 2 4 の記録再生装置 4 0 1および図 3 1 の記録再生装置 5 0 1は、図 3 4 に示されるような記録再生装置 6 0 1によ
- 25    トウェアにより実行させることもできる。この場合、例えば、図 4 の記録再生装置 1 0 1、図 2 1 の記録再生装置 3 0 1、図 2 4 の記録再生装置 4 0 1および図 3 1 の記録再生装置 5 0 1は、図 3 4 に示されるような記録再生装置 6 0 1によ

り構成される。

図 3 1 において、CPU (Central Processing Unit) 6 1 1 は、ROM (Read Only Memory) 6 1 2 に記憶されているプログラム、または、HDD 6 1 9 から RAM (Random Access Memory) 6 1 3 にロードされたプログラムに従って  
5 各種の処理を実行する。RAM 6 1 3 にはまた、CPU 6 1 1 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

CPU 6 1 1、ROM 6 1 2、およびRAM 6 1 3 は、バス 6 1 4 を介して相互に接続されている。このバス 6 1 4 にはまた、入出力インタフェース 6 1 5 も接続されている。

10 入出力インタフェース 6 1 5 には、コンテンツの入出力の制御を行う AV ボード 6 1 6、キーボード、マウスなどよりなる入力部 6 1 7、CRT (Cathode Ray Tube), LCD (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどよりなる出力部 6 1 8、HDD 6 1 9、モデム、ターミナルアダプタなどより構成される通信部 6 2 0 が接続されている。通信部 6 2 0 は、バス  
15 や図示しないネットワークを介しての通信処理を行う。

入出力インタフェース 6 1 5 にはまた、必要に応じてドライブ 6 3 0 が接続され、磁気ディスク 6 3 1、光ディスク 6 3 2、光磁気ディスク 6 3 3、或いは半導体メモリ 6 3 4 などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて HDD 6 1 9 にインストールされる。

20 一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば、汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

25 この記録媒体は、図 3 4 に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 6 3 1 (フレキシブルディスクを含む)、光ディスク 6 3 2 (CD-ROM (Compact Dis

k-Read Only Memory), DVD(Digital Versatile Disk)を含む)、光磁気ディスク 6 3 3 (MD(Mini-Disk) (商標)を含む)、もしくは半導体メモリ 6 3 4 などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM 6 1 2 や、HDD 6 1 9 などで構成される。

なお、コンテンツおよび保護情報などを記録もしくは再生する図 4 の光ディスク 1 4 1 が、例えば、DVD の他、CD-R その他の光ディスク、MD その他の光磁気ディスク、磁気ディスク等のディスク型の記録媒体である場合、ディスク表面に同心円状またはスパイラル状に設定された「トラック」の上に、ピットまたはマークをデータの記録波形に基づいて形成することにより、情報が記録されるようになされている。

例えば、CD-ROM や DVD-ROM など、プレスしてデータを記録するメディアでは、実際に表面に物理的なくぼみであるピットが形成される。これに対し、例えば、CD-R、CD-RW、DVD-R、DVD-RW、または、DVD-RAM などの追記または書き換え型のメディアの場合、物理的なくぼみをつける代わりに、レーザ光を当て、その熱によってメディア内部の相変化膜に化学変化を生じさせることにより、くぼみの代用であるマークが形成される。

記録されたデータが再生される場合、データを読み取るためにヘッドから照射されたレーザ光は、メディア表面で反射するが、その際、このピットまたはマークの有無によって反射光に変化が生じることによりデータが再生される。

記録されているデータの認識方法には、ピットの有無がビットデータを表す「マークポジション記録方式」と、ピットの存在がビットを反転させる「マークエッジ記録方式」が存在する。

後者は、反射率が一定の状態で読み取られたピットを「0」、反射率がピット中で変化したピットを「1」と認識する方式で、データを記録する際のトラックのロスを少なくし、ピット長を縮めることに貢献している。

なお、図 3 4 を参照して上述した磁気ディスク 6 3 1、光ディスク 6 3 2、光

磁気ディスク 6 3 3、ROM 6 1 2、または、HDD 6 1 9などのディスク型の記録媒体における情報の記録または再生の方法も、図 4 の光ディスク 1 4 1 がディスク型の記録媒体である場合と同様である。

- 5      なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

        なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

10

#### 産業上の利用可能性

        以上の如く、本発明によれば、保護の要不要に基づいて、コンテンツを柔軟に保護することができる。また、本発明によれば、コンテンツの不正コピーが抑制される。さらに、本発明によれば、PCストレージ運用が可能になる。

## 請求の範囲

1. 入力装置と記録装置がバスを介して接続された記録システムにおいて、  
前記入力装置は、入力されたコンテンツを保護するか否かを判断する判断手段を備え、
- 5 前記記録装置は、前記判断手段により判断された結果に基づいて、前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かを示す保護情報を、前記コンテンツとともに記録媒体に記録する記録手段を備える  
ことを特徴とする記録システム。
2. 前記記録手段は、前記コンテンツの所定の単位ごとに前記保護情報を記録  
10 する  
ことを特徴とする請求の範囲第1項に記載の記録システム。
3. 前記所定の単位は、2048バイトである  
ことを特徴とする請求の範囲第2項に記載の記録システム。
4. 前記記録装置は、前記判断手段により前記コンテンツを保護すると判断さ  
15 れた場合、前記記録媒体のIDと記録媒体鍵を作用させて前記コンテンツを暗号化  
する暗号化手段をさらに備える  
ことを特徴とする請求の範囲第1項に記載の記録システム。
5. 前記記録装置は、前記判断手段により前記コンテンツを保護しないと判断  
された場合、少なくとも、前記記録媒体の記録媒体鍵を作用させて前記コンテ  
20 ツを暗号化する暗号化手段をさらに備える  
ことを特徴とする請求の範囲第1項に記載の記録システム。
6. 前記入力装置および前記記録装置は、それぞれ相互に認証する認証手段を  
さらに備える  
ことを特徴とする請求の範囲第1項に記載の記録システム。
- 25 7. 前記入力装置は、前記判断手段により前記コンテンツを保護すると判断さ  
れた場合、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化す  
る第1の暗号化手段をさらに備え、



前記記録装置は、前記判断手段により前記コンテンツを保護すると判断された場合、前記記録手段による前記コンテンツの記録前に、前記コンテンツを暗号化する第 2 の暗号化手段をさらに備える

ことを特徴とする請求の範囲第 1 項に記載の記録システム。

- 5    8.    前記判断手段により前記コンテンツを保護しないと判断された場合、前記第 1 の暗号化手段は、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化することを禁止する

ことを特徴とする請求の範囲第 7 項に記載の記録システム。

9.    入力装置と記録装置がバスを介して接続された記録システムの記録方法に  
10    おいて、

前記入力装置は、入力されたコンテンツを保護するか否かを判断し、

前記記録装置は、判断された結果に基づいて、前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を、前記コンテンツとともに記録媒体に記録する

- 15    ことを特徴とする記録方法。

10.    記録媒体に情報を記録する記録装置において、

バスを介して接続された他の装置と相互に認証を行う認証手段と、

前記他の装置から前記バスを介して供給される第 1 の暗号化方法により暗号化されたコンテンツを復号する復号手段と、

- 20    前記復号手段により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録手段と

を備えることを特徴とする記録装置。

11.    前記復号された前記コンテンツを、第 2 の暗号化方法により暗号化する  
25    暗号化手段をさらに備える

ことを特徴とする請求の範囲第 10 項に記載の記録装置。

12.    前記暗号化手段は、前記記録媒体の ID と記録媒体鍵を作用させて前記

復号されたコンテンツを暗号化する

ことを特徴とする請求の範囲第 11 項に記載の記録装置。

13. 前記記録手段は、前記他の装置から前記バスを介して供給された前記コンテンツが、前記第 1 の暗号方法により暗号化されていないコンテンツの場合、

5 前記コンテンツを、前記バス上での伝送において保護すべきコンテンツでないことを示す保護情報とともに記録する

ことを特徴とする請求の範囲第 10 項に記載の記録装置。

14. 記録媒体に情報を記録する記録装置の記録方法において、  
バスを介して接続された他の装置と相互に認証を行う認証ステップと、

10 前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

15 を含むことを特徴とする記録方法。

15. 記録媒体に情報を記録する記録装置用のプログラムであって、  
バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号する復号ステップと、

20 前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

25 16. 記録媒体に情報を記録する記録装置のプログラムであって、  
バスを介して接続された他の装置と相互に認証を行う認証ステップと、  
前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号

する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

5       を含むことを特徴とするプログラム。

17.   コンテンツが入力される入力装置において、

バスを介して接続された記録装置と相互に認証を行う認証手段と、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを第1の暗号化方法で暗号化する第1

10   の暗号化手段と、

前記第1の暗号化手段により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給手段と

を備えることを特徴とする入力装置。

18.   前記第1の暗号化手段により暗号化された前記コンテンツを、第2の暗

15   号化方法で暗号化する第2の暗号化手段を

さらに備えることを特徴とする請求の範囲第17項に記載の入力装置。

19.   前記第1の暗号化手段および前記第2の暗号化手段のうちの一方は、記録媒体のIDと記録媒体鍵を作用させて前記コンテンツを暗号化する

ことを特徴とする請求の範囲第18項に記載の入力装置。

20   20.   コンテンツが入力される入力装置の入力方法において、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを

25   介して前記記録装置に供給する供給ステップと

を含むことを特徴とする入力方法。

21.   コンテンツが入力される入力装置用のプログラムであって、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、  
入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、  
前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

22. コンテンツが入力される入力装置のプログラムであって、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、

10 入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと

を含むことを特徴とするプログラム。

15 23. 再生装置と出力装置がバスを介して接続された再生システムにおいて、

前記再生装置は、記録媒体からコンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、

20 前記再生手段により再生された前記保護情報に基づいて、前記バス上の前記出力装置への前記コンテンツの送出を制御する送出制御手段とを備え、

前記出力装置は、前記送出制御手段により送出された前記コンテンツを外部に出力する出力手段を備える

ことを特徴とする再生システム。

24. 前記保護情報は、前記コンテンツの所定の単位ごとに記録されている

25 ことを特徴とする請求の範囲第23項に記載の再生システム。

25. 前記所定の単位は、2048バイトである

ことを特徴とする請求の範囲第24項に記載の再生システム。

26. 前記再生装置は、前記再生手段により再生されたコンテンツを復号する復号手段をさらに備える

ことを特徴とする請求の範囲第23項に記載の再生システム。

27. 前記再生装置は、前記バス上の装置を認証する認証手段をさらに備える

5 ことを特徴とする請求の範囲第23項に記載の再生システム。

28. 前記再生装置は、前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記バス上の前記出力装置が認証されている場合、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する暗号化手段をさらに備え、

10 前記出力装置は、前記暗号化手段により暗号化された前記コンテンツを復号する第1の復号手段をさらに備える

ことを特徴とする請求の範囲第27項に記載の再生システム。

29. 前記出力装置は、前記第1の復号手段により復号された前記コンテンツを、前記記録媒体のIDと記録媒体鍵を作用させて復号する第2の復号手段をさらに備える

15

ことを特徴とする請求の範囲第28項に記載の再生システム。

30. 前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記バス上の装置が認証されていない場合、前記送出制御手段は、前記バス上の装置への前記コンテンツの送出を禁止する

20

ことを特徴とする請求の範囲第27項に記載の再生システム。

31. 再生装置と出力装置がバスを介して接続された再生システムの再生方法において、

前記再生装置は、記録媒体からコンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生し、再生された前記保護情報に基づいて、前記バス上の前記出力装置への前記コンテンツの送出を制御し、

25

前記出力装置は、前記再生装置から送出された前記コンテンツを外部に出力する

ことを特徴とする再生方法。

3 2. コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置において、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、

10 前記再生手段により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御手段とを備えることを特徴とする再生装置。

3 3. 前記保護情報は、前記コンテンツの所定の単位ごとに記録されていることを特徴とする請求の範囲第 3 2 項に記載の再生装置。

3 4. 前記所定の単位は、2 0 4 8 バイトであることを特徴とする請求の範囲第 3 3 項に記載の再生装置。

3 5. 前記他の装置を認証する認証手段と、

前記コンテンツを暗号化する暗号化手段とをさらに備え、

20 前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記他の装置が認証されている場合、前記暗号化手段は、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する

ことを特徴とする請求の範囲第 3 2 項に記載の再生装置。

3 6. 前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記他の装置が  
25 認証されていない場合、前記出力制御手段は、前記バスへの前記コンテンツの出力を禁止する

ことを特徴とする請求の範囲第 3 5 項に記載の再生装置。

37. コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置の再生方法において、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とする再生方法。

10 38. コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置用のプログラムであって、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

15 前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

20 39. コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置のプログラムにおいて、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

25 前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とするプログラム。



図 1

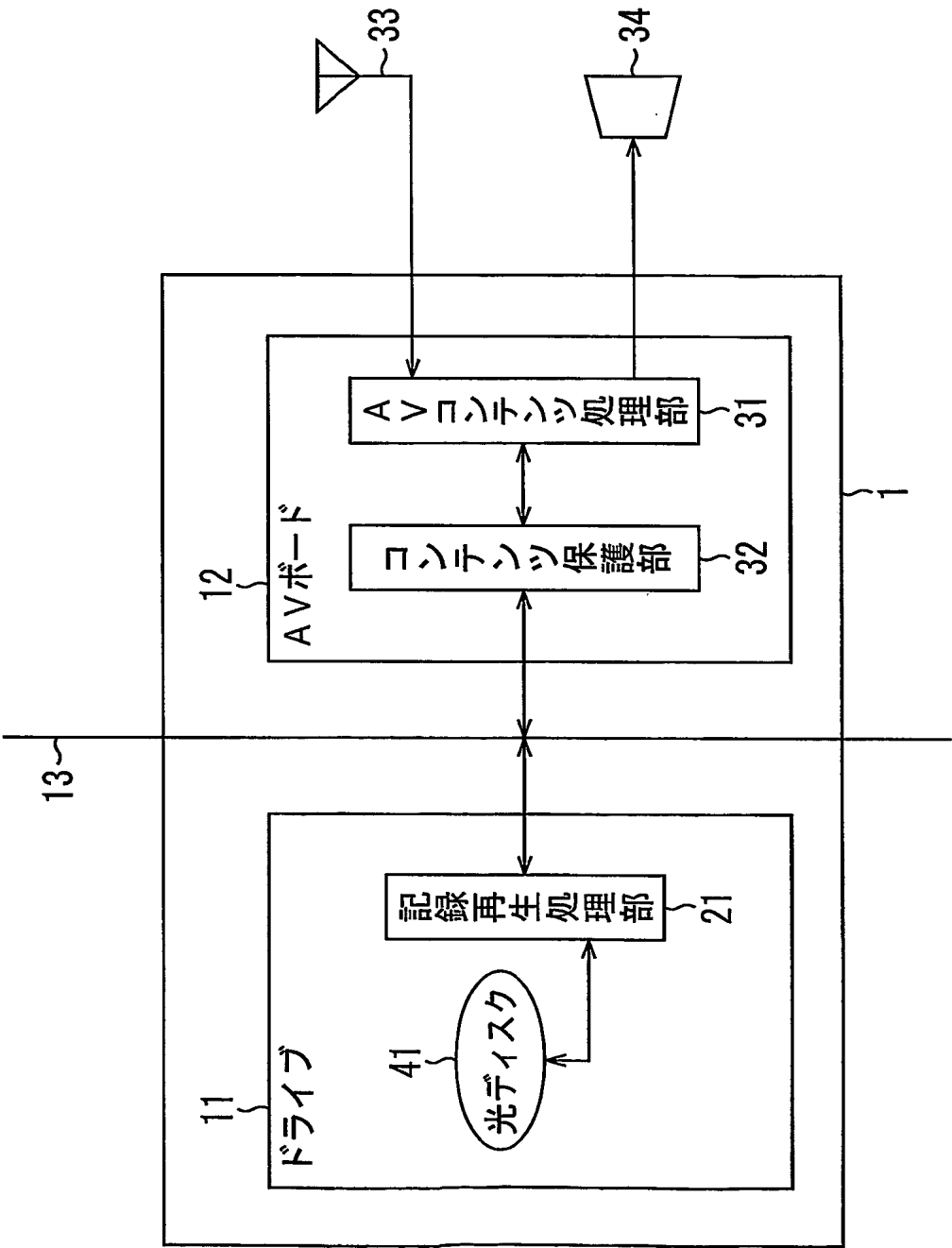


図2

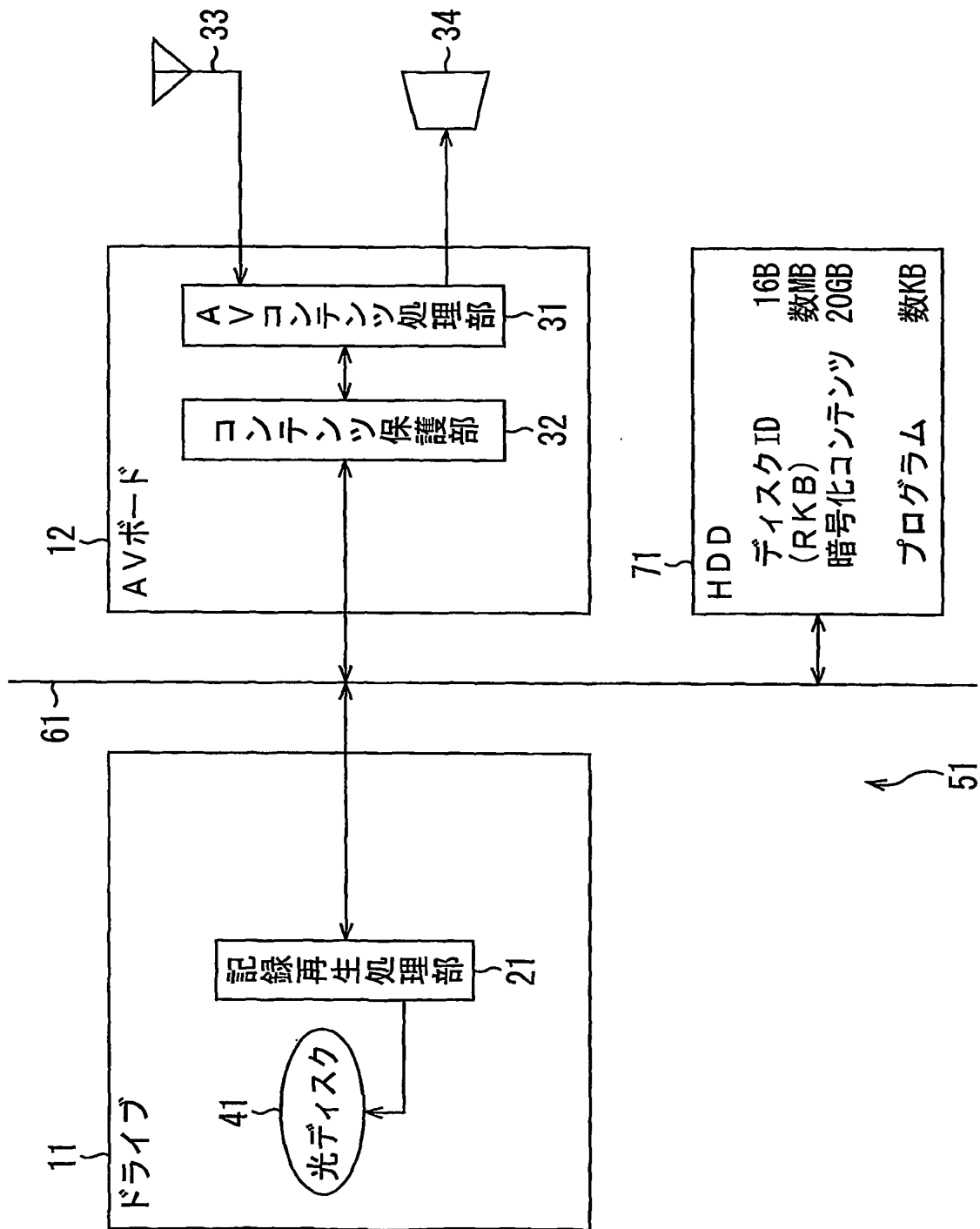
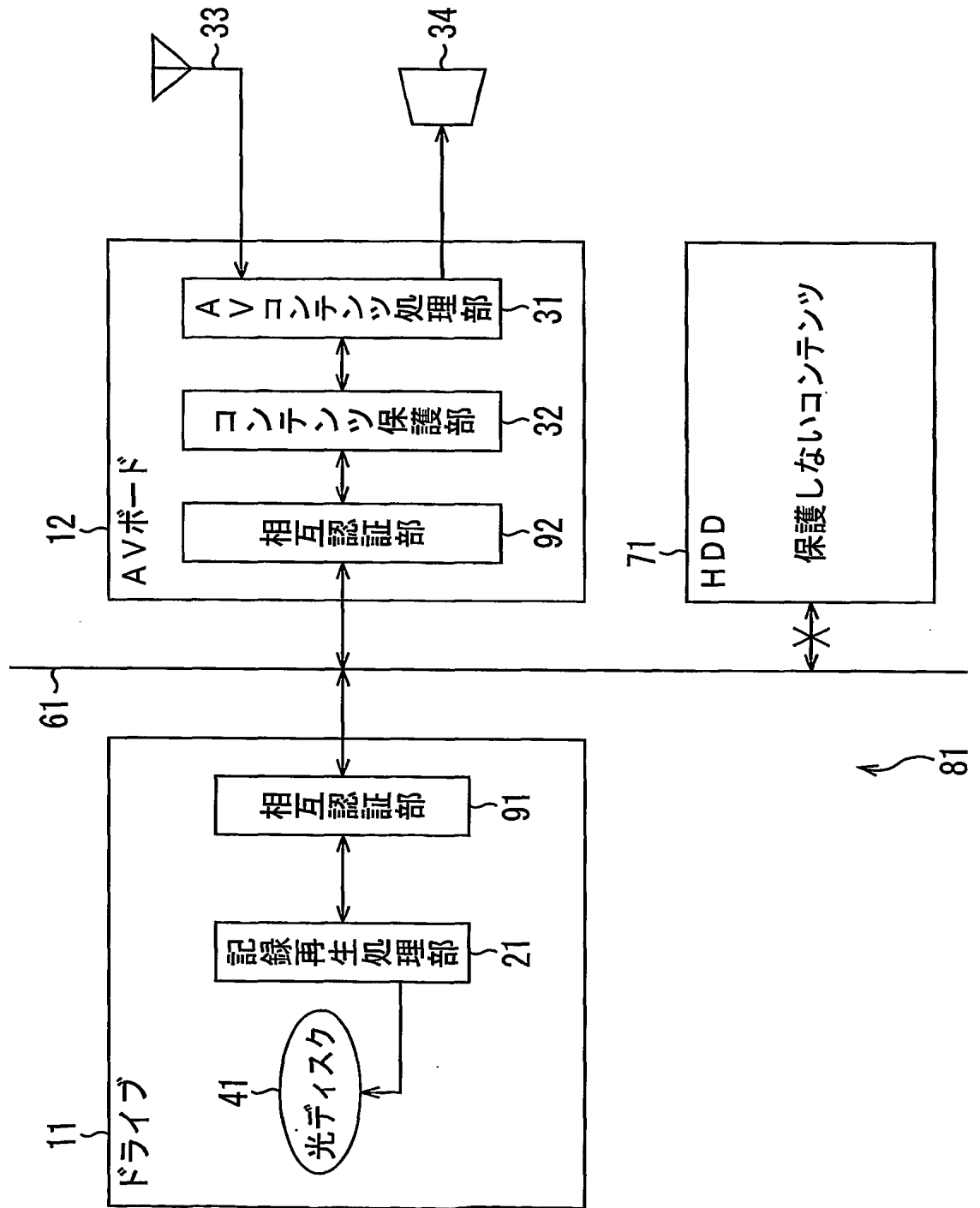
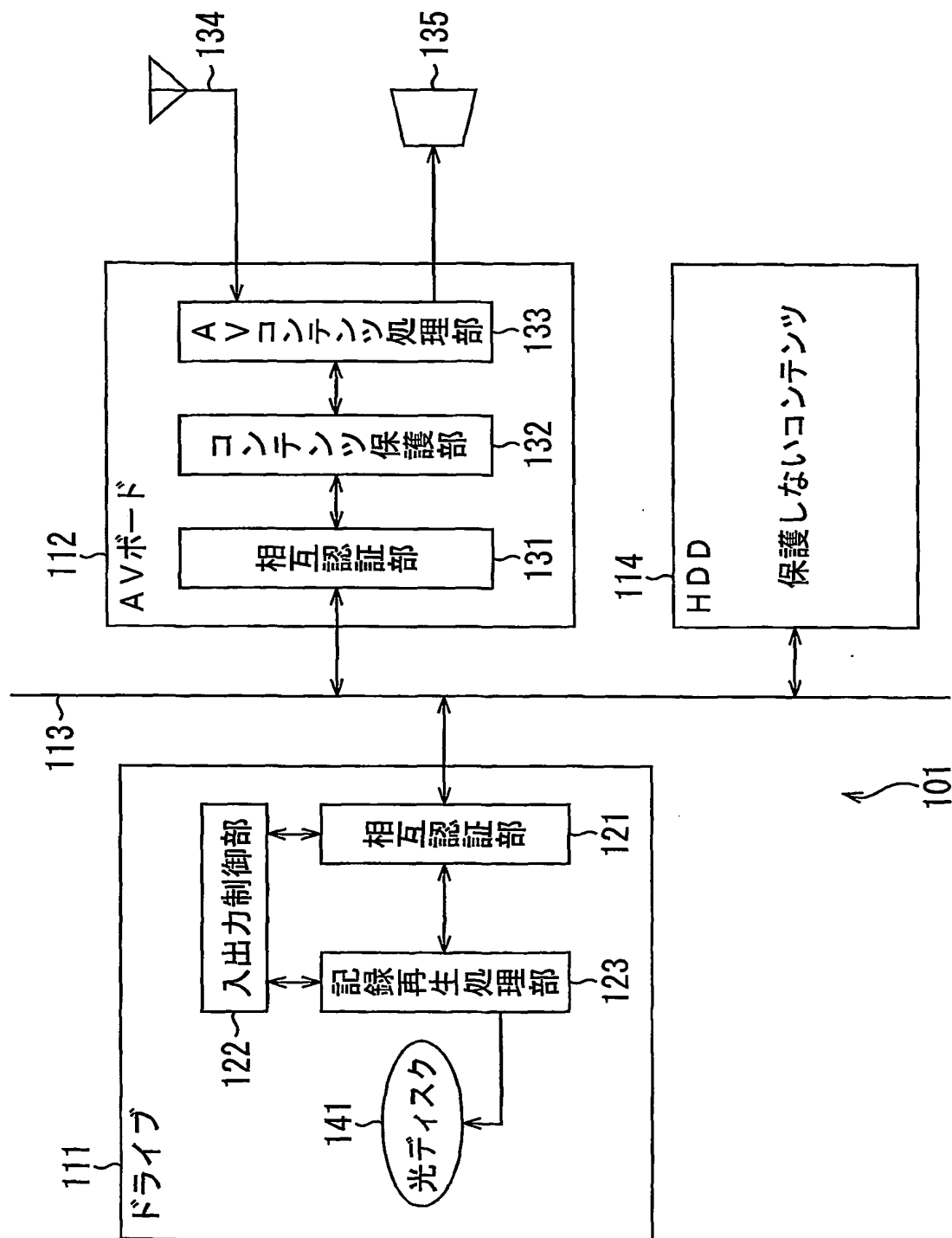


図3



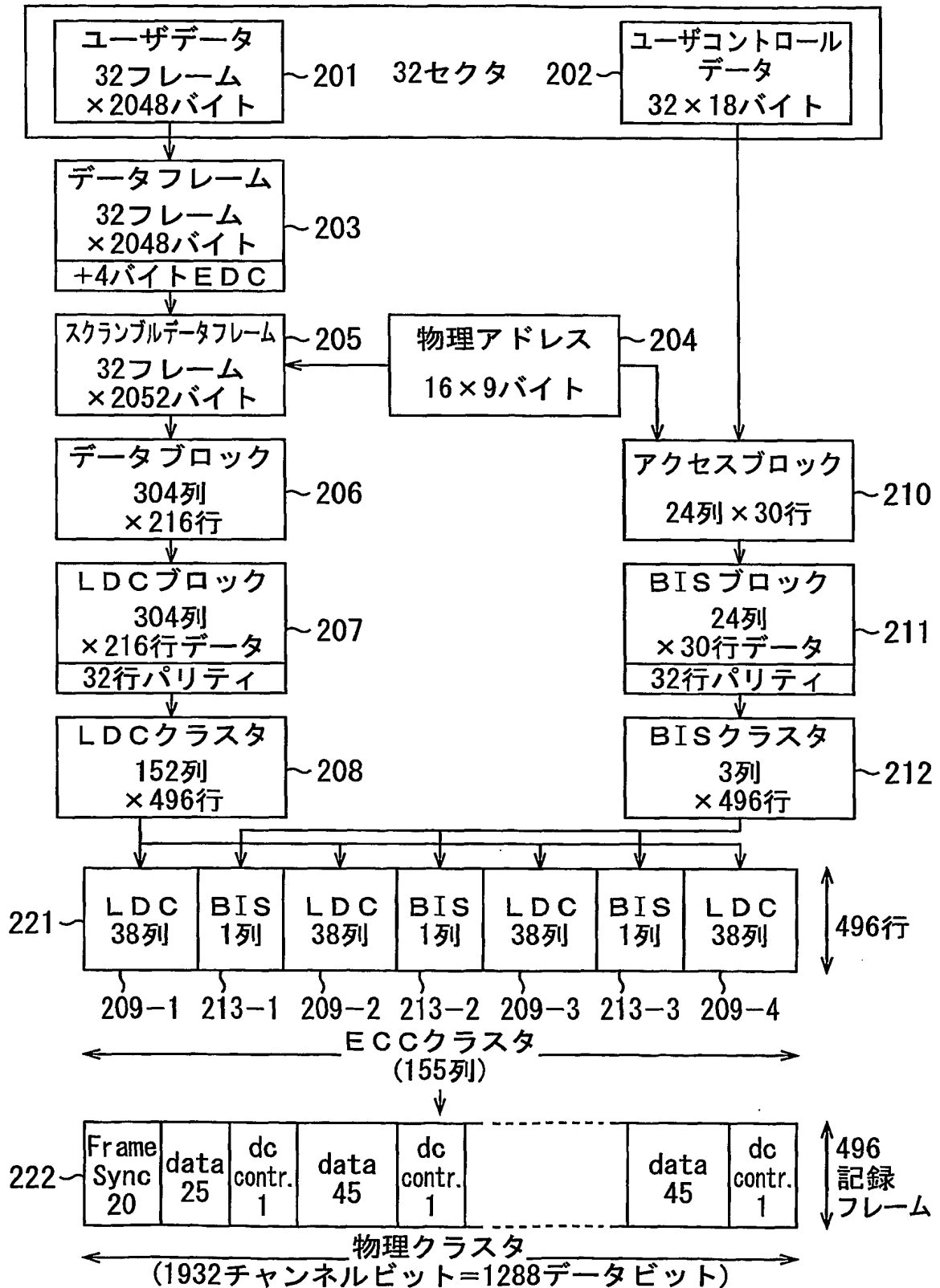
4/33

図4



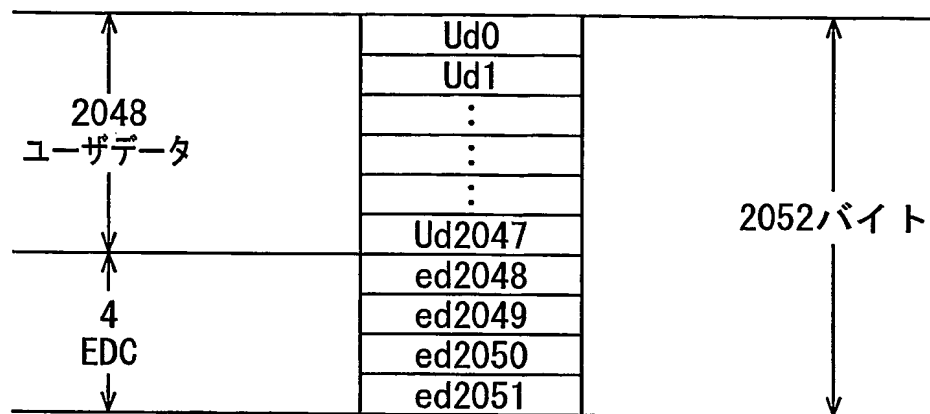
5/33

図 5



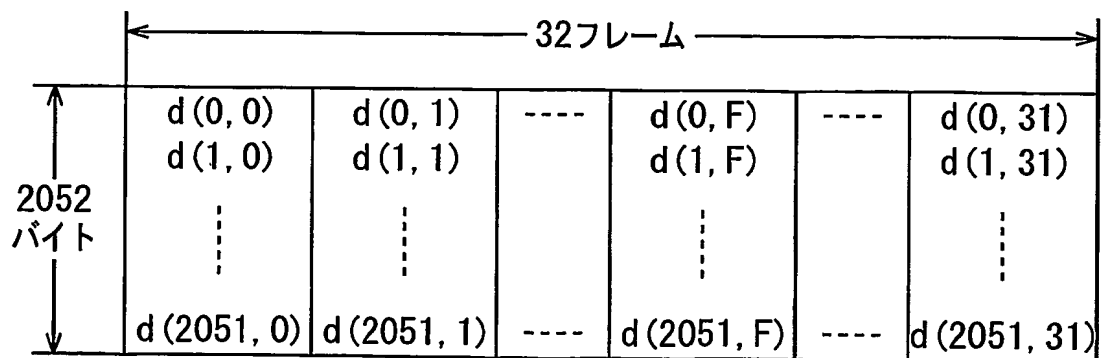
6/33

図 6



203

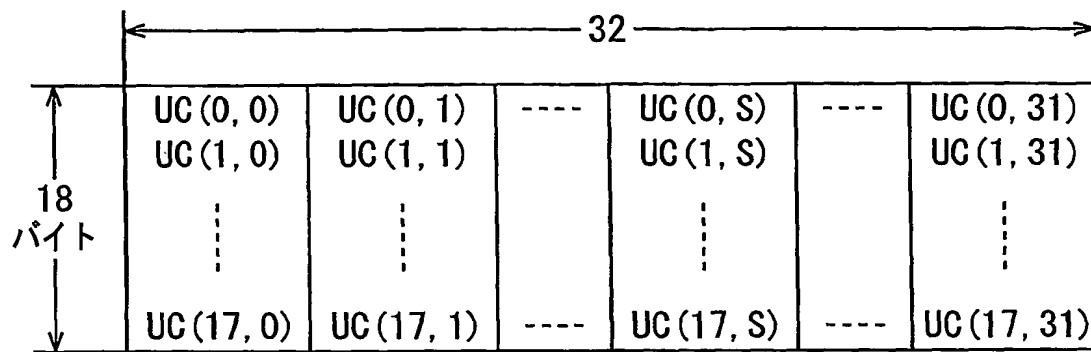
図 7



205

7/33

図 8



202

図 9

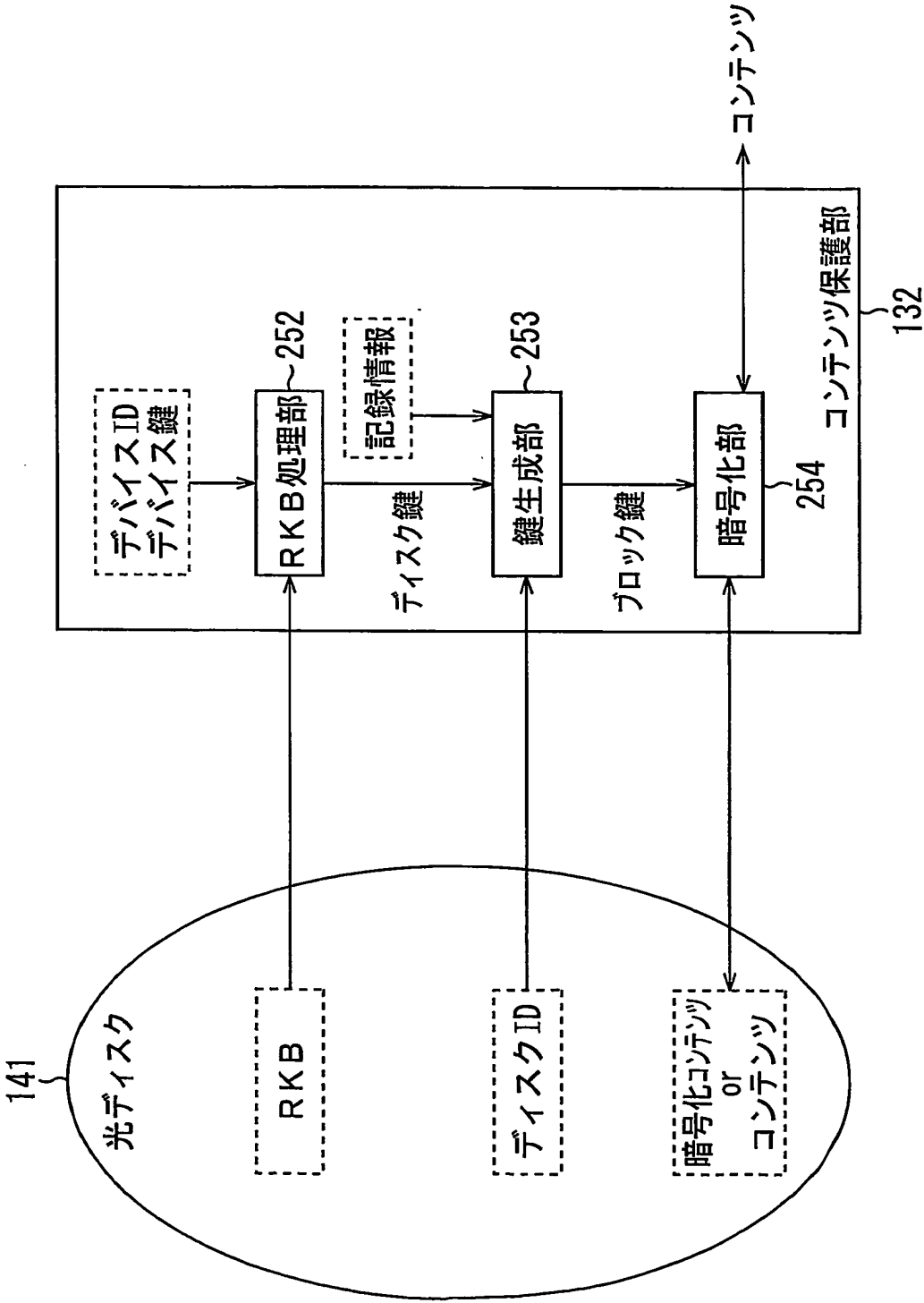
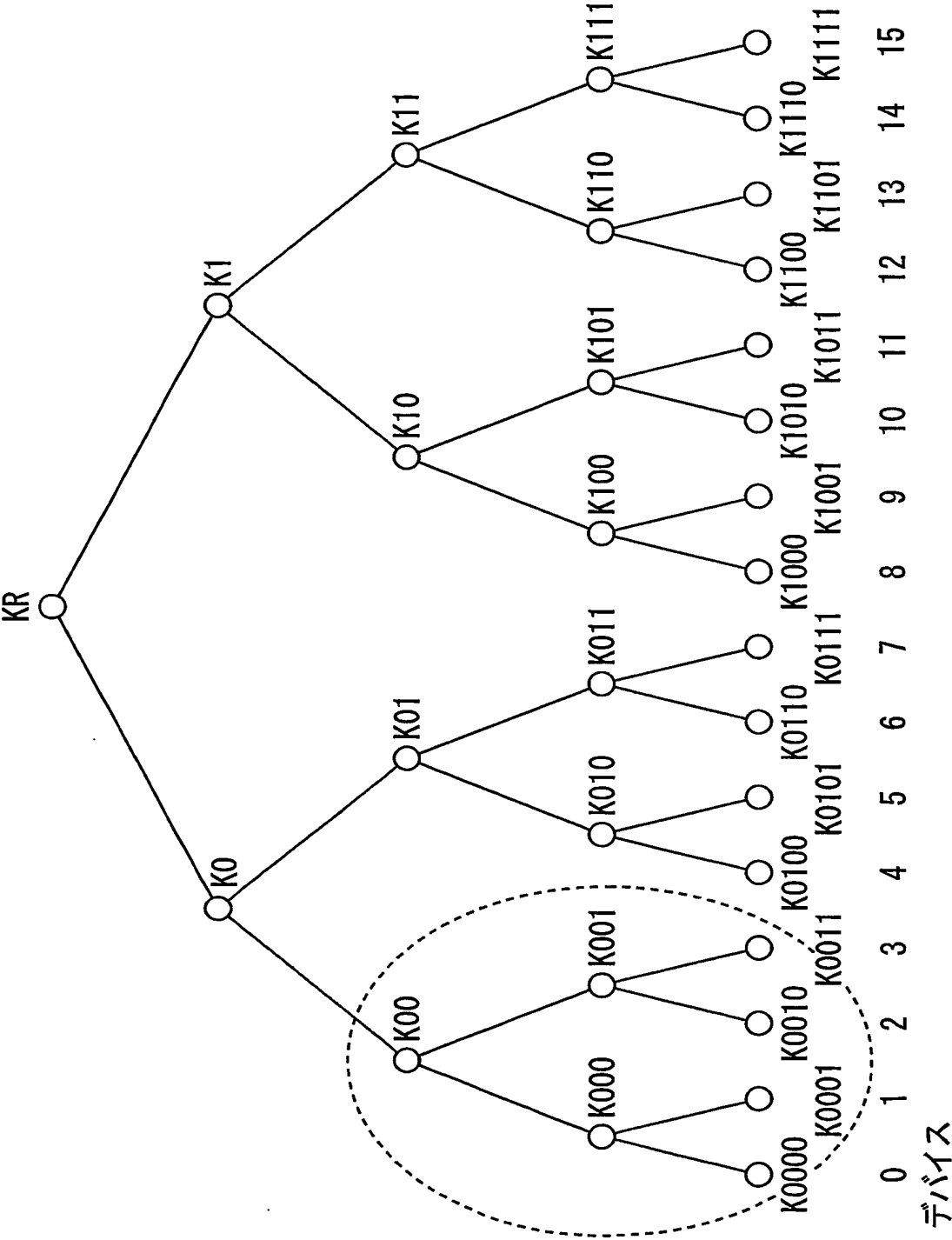




図10



10/33

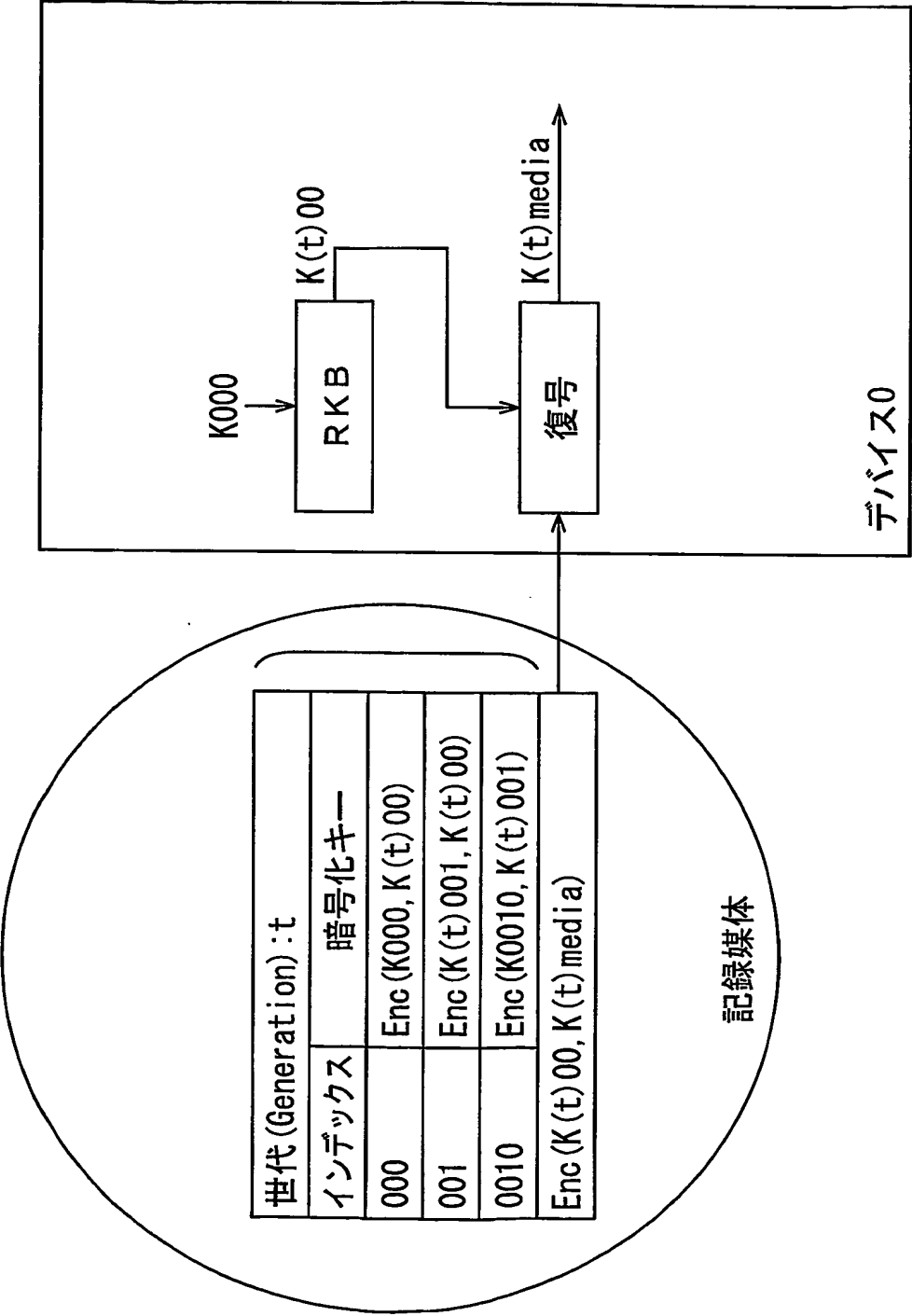
図11 A

バージョン (Version) : t	
インデックス	暗号化キー
0	Enc (K (t) 0, K (t) R)
00	Enc (K (t) 00, K (t) 0)
000	Enc (K000, K (t) 00)
001	Enc (K (t) 001, K (t) 00)
0010	Enc (K0010, K (t) 001)

図11 B

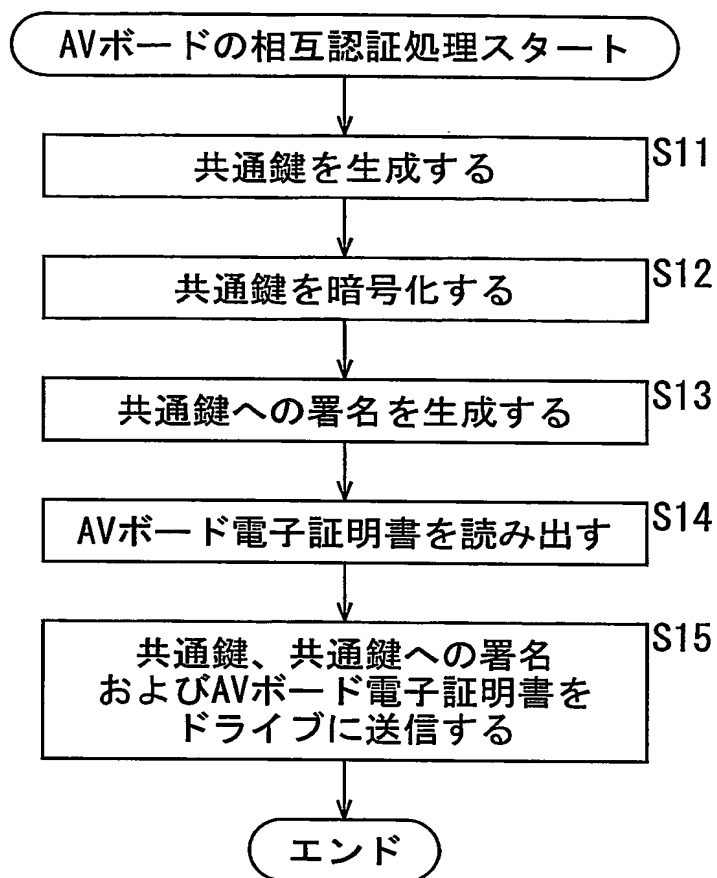
バージョン (Version) : t	
インデックス	暗号化キー
000	Enc (K000, K (t) 00)
001	Enc (K (t) 001, K (t) 00)
0010	Enc (K0010, K (t) 001)

図12



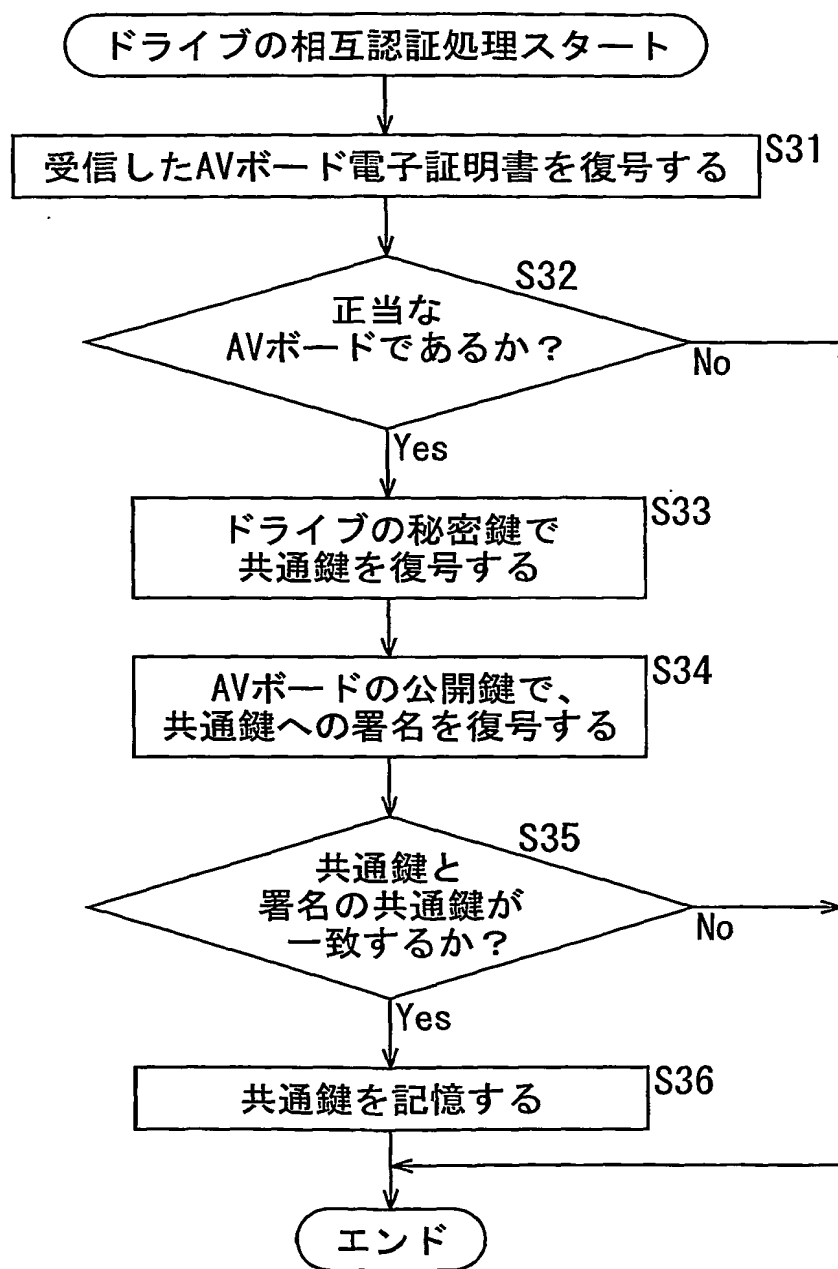
12/33

図13



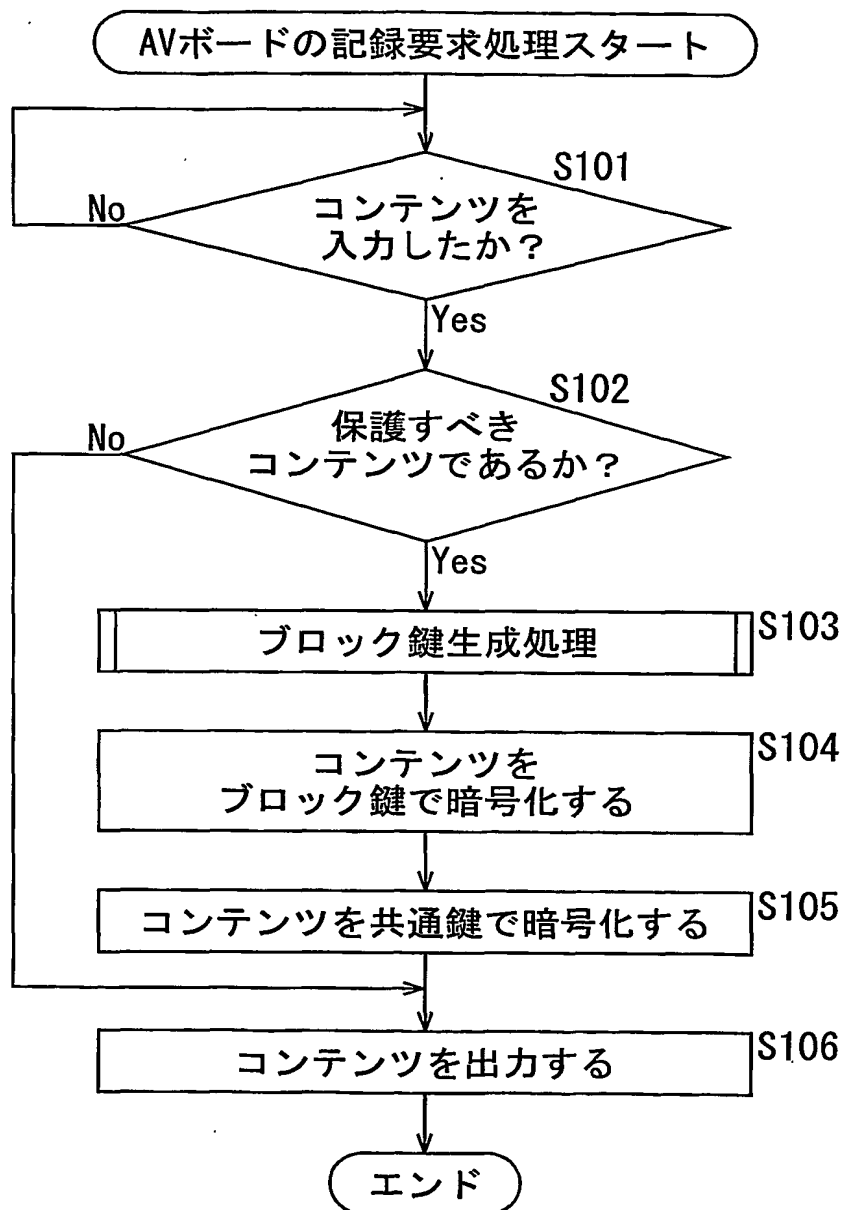
13/33

図14



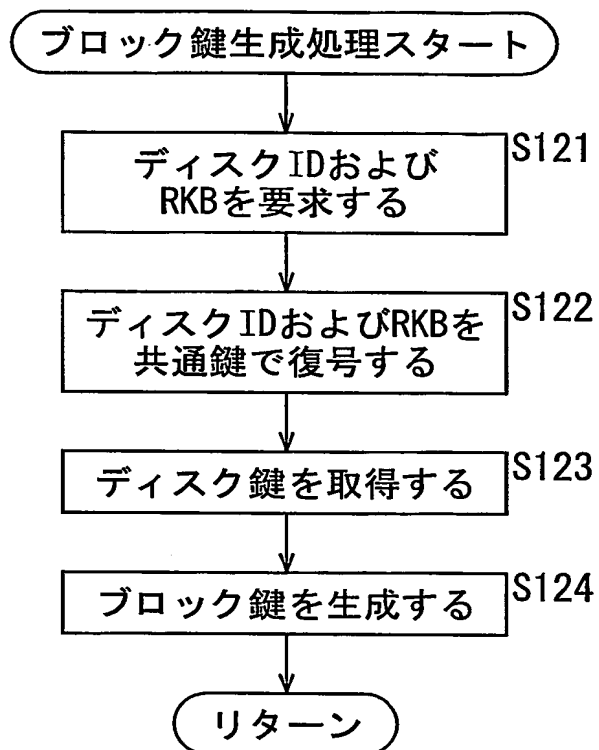
14/33

図15



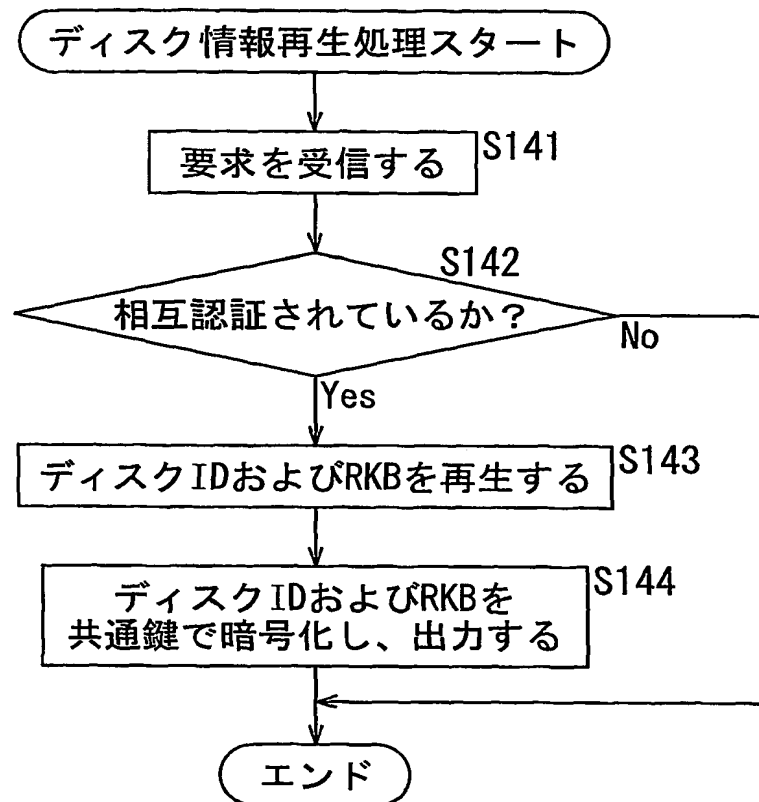
15/33

図16



16/33

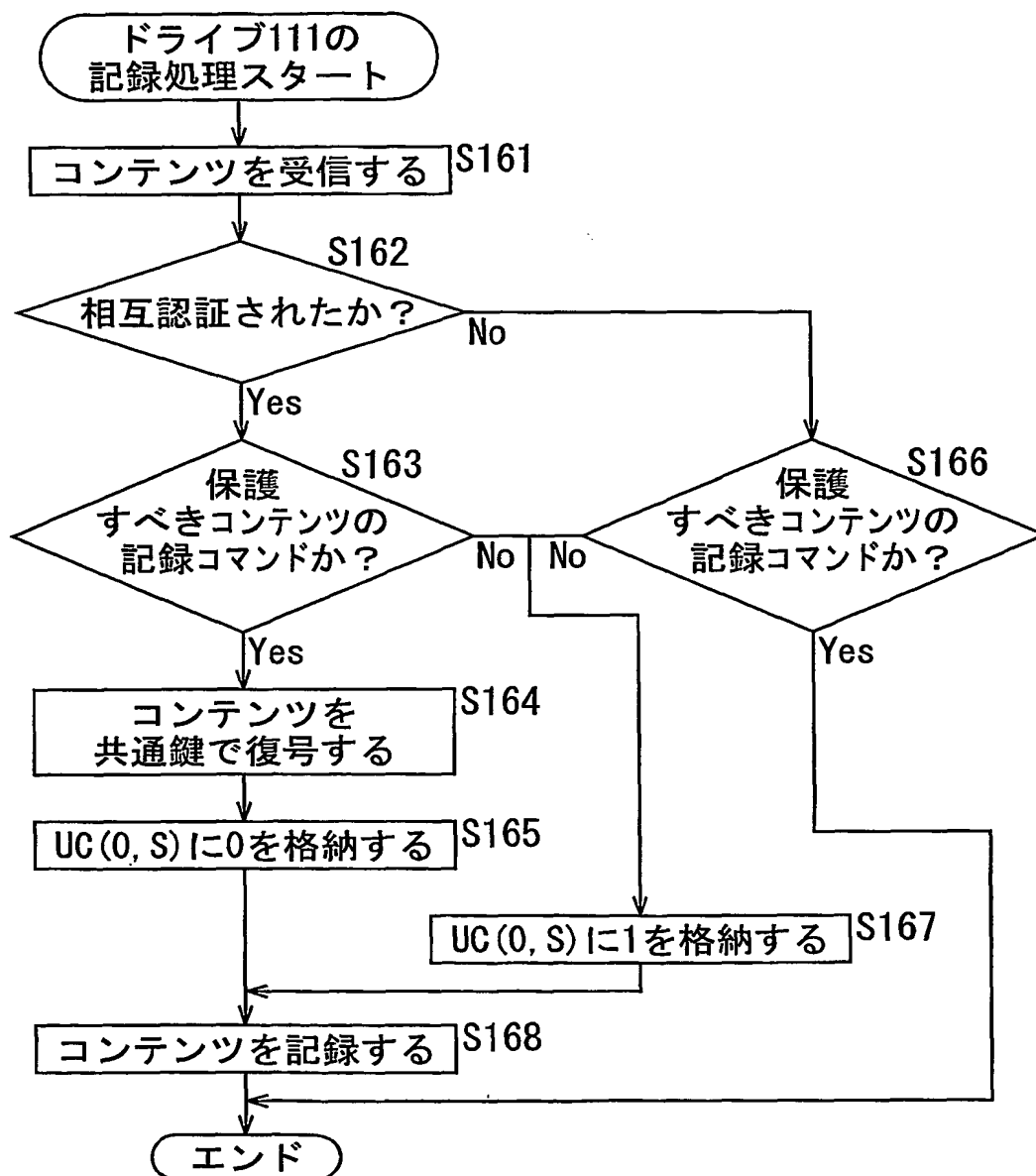
図17





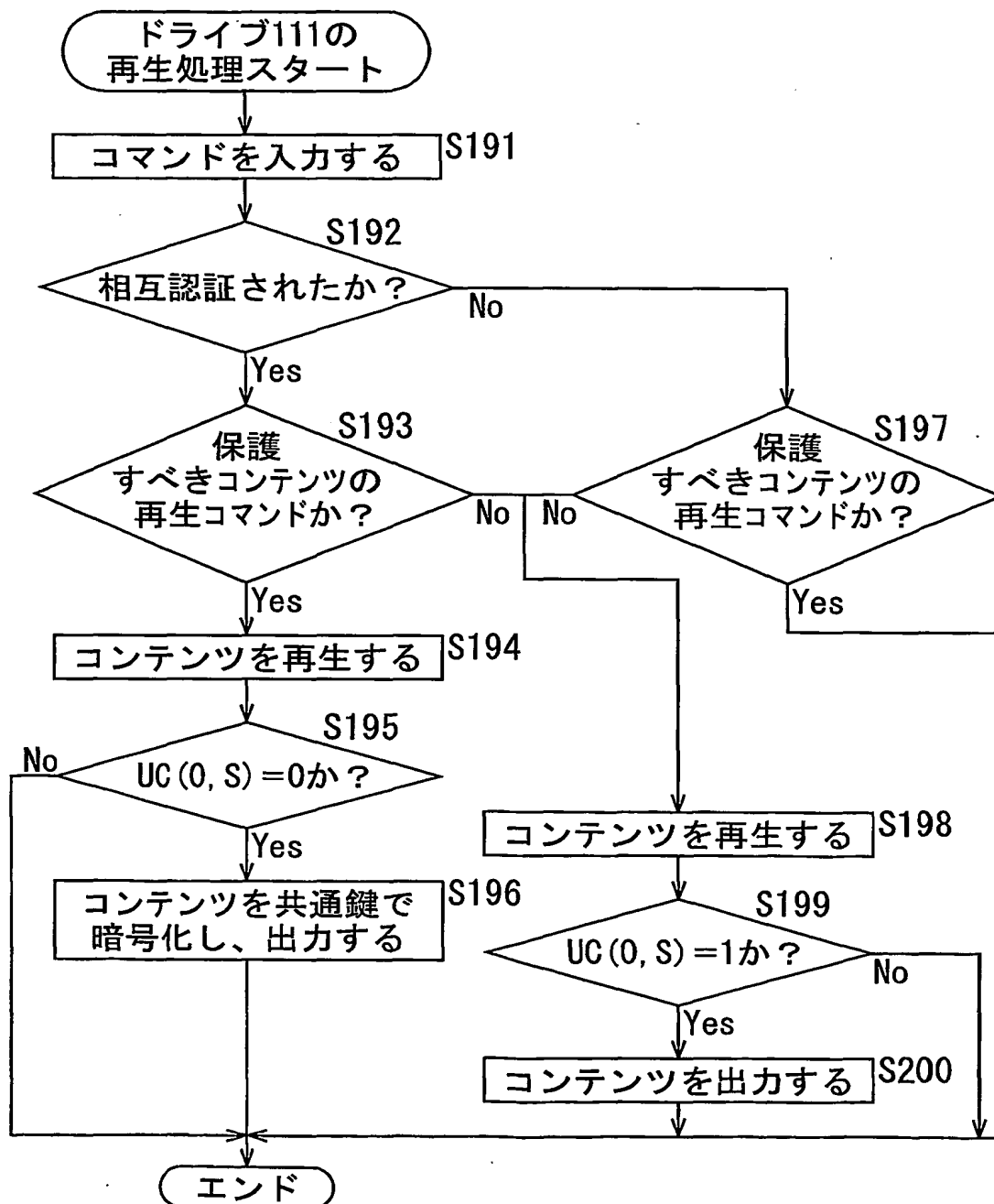
17/33

図18



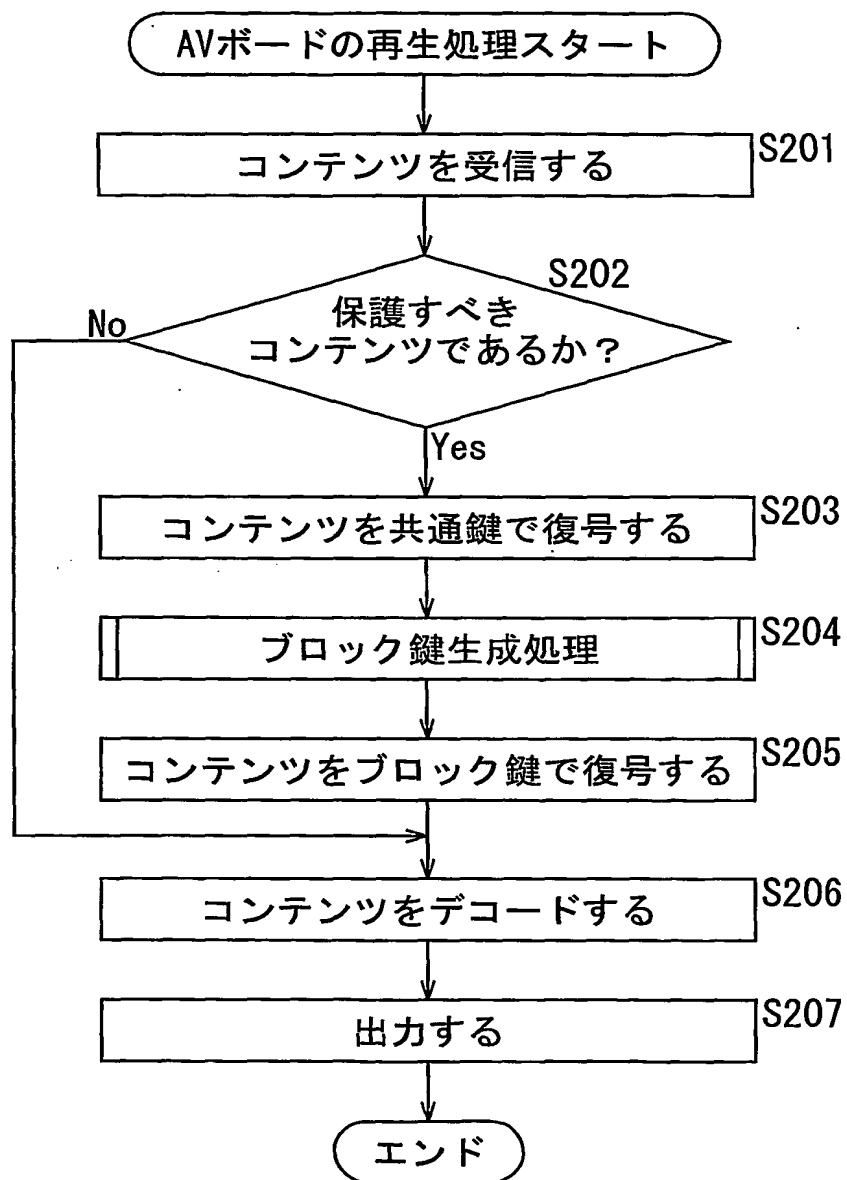
18/33

図19



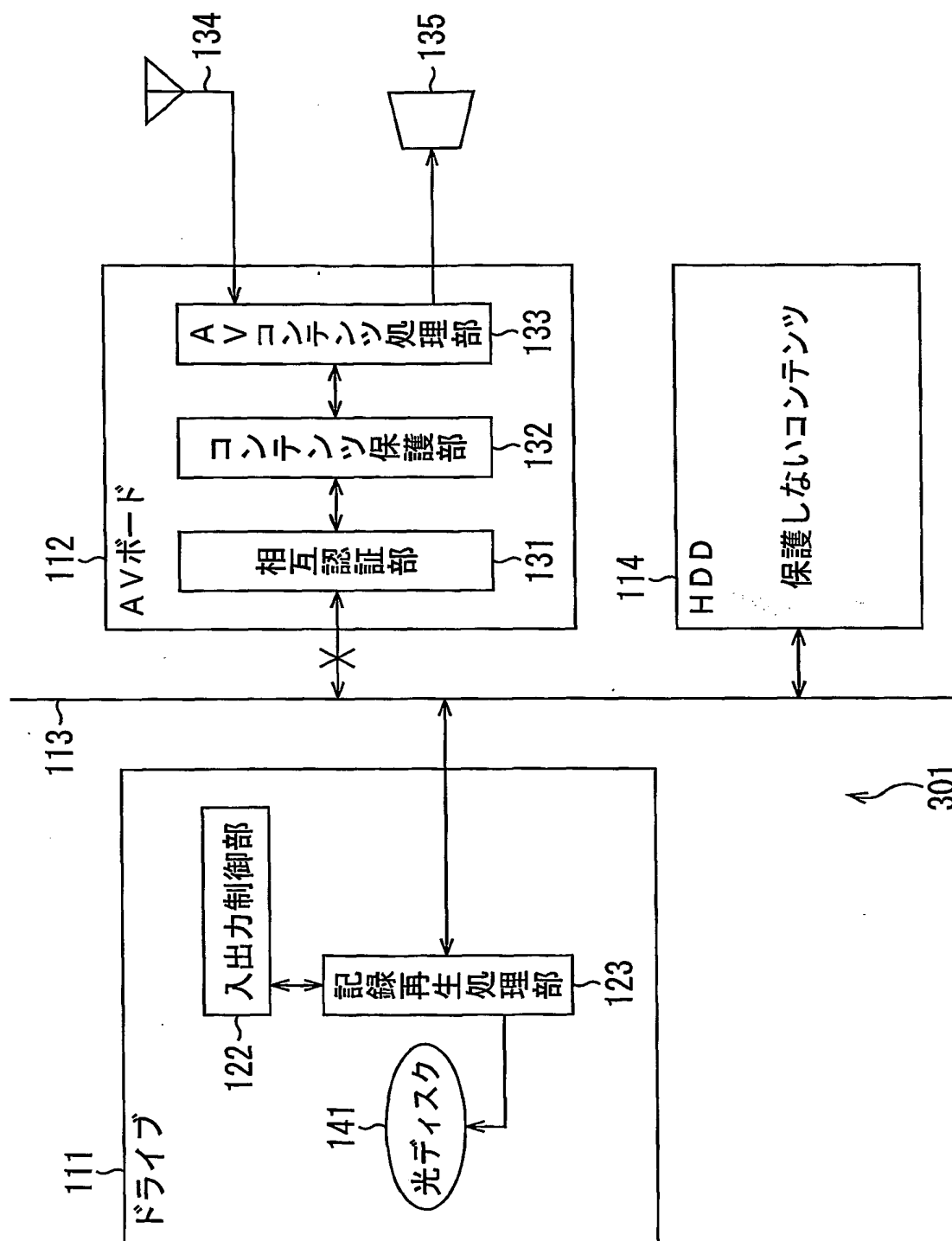
19/33

図20



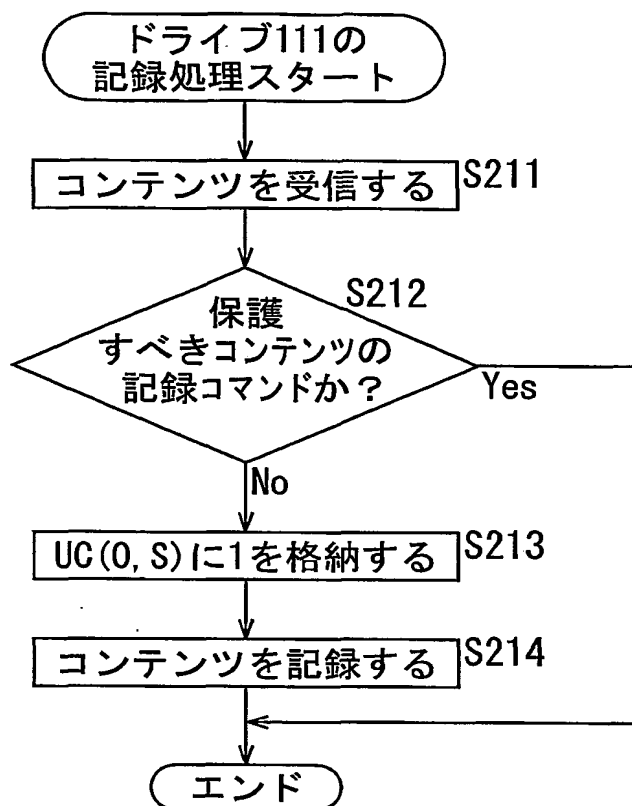
20/33

図21



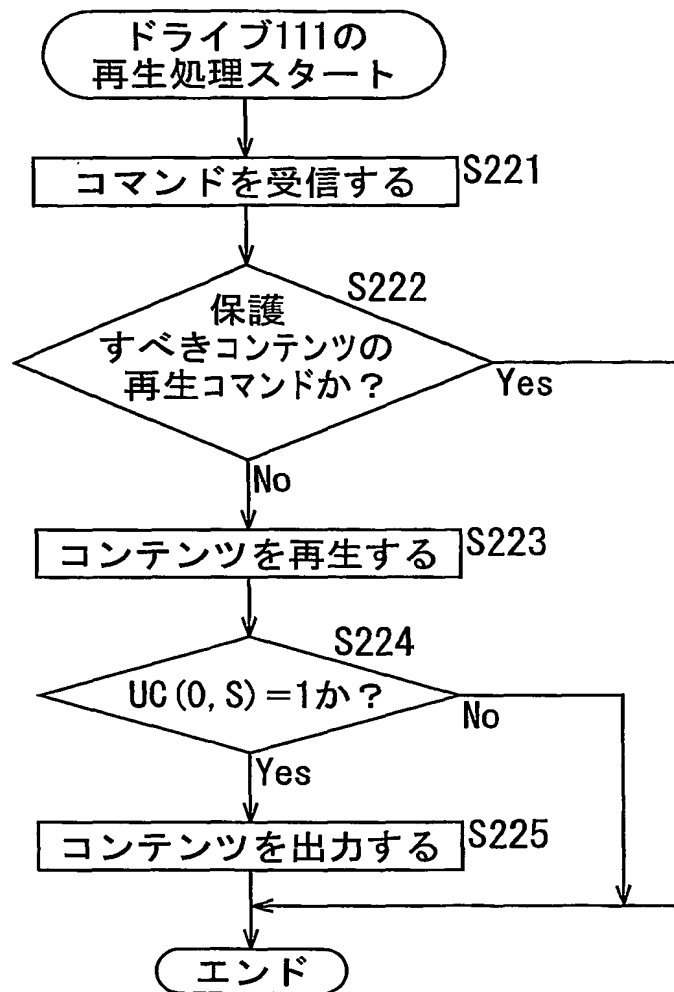
21/33

図22



22/33

図23



23/33

図24

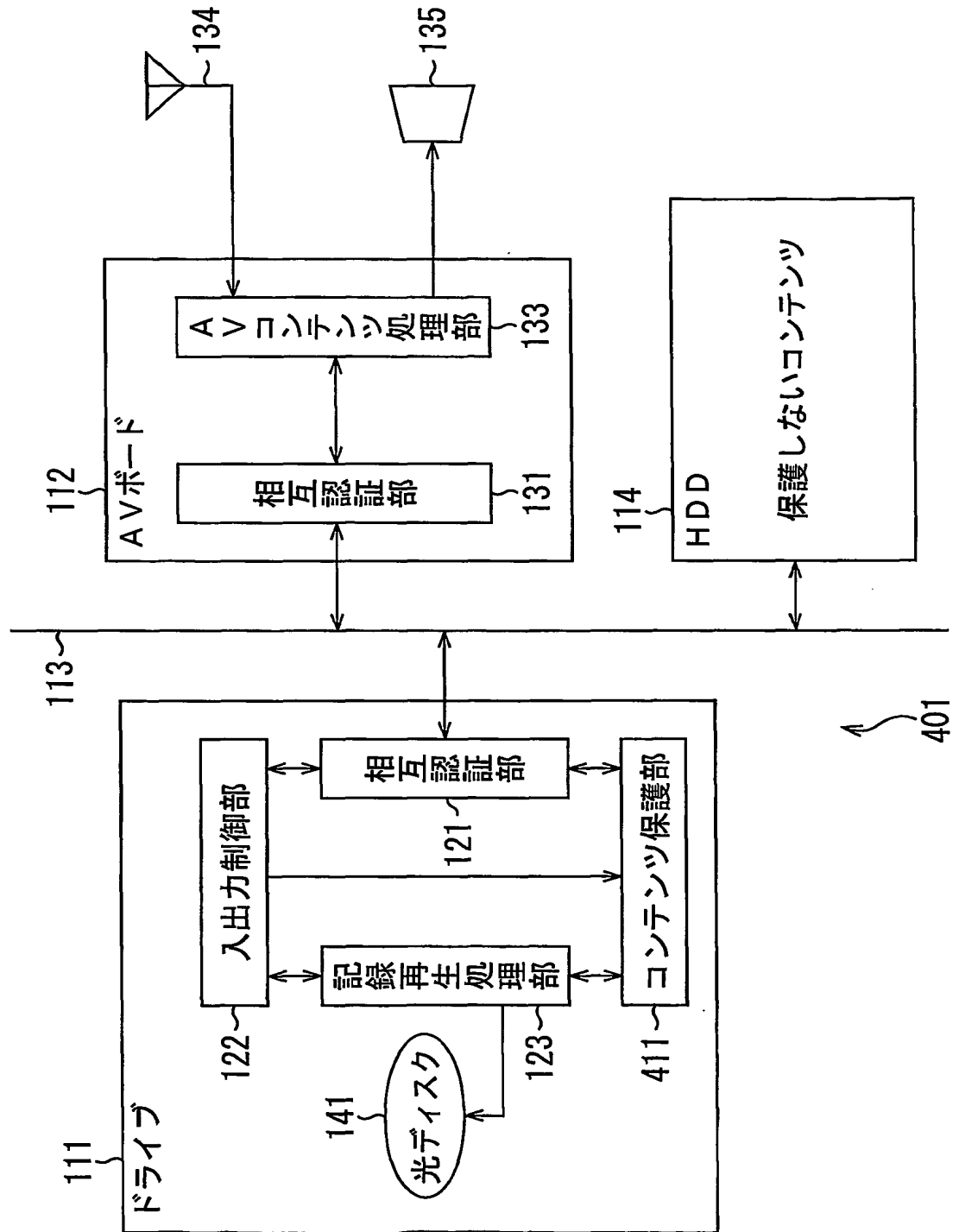
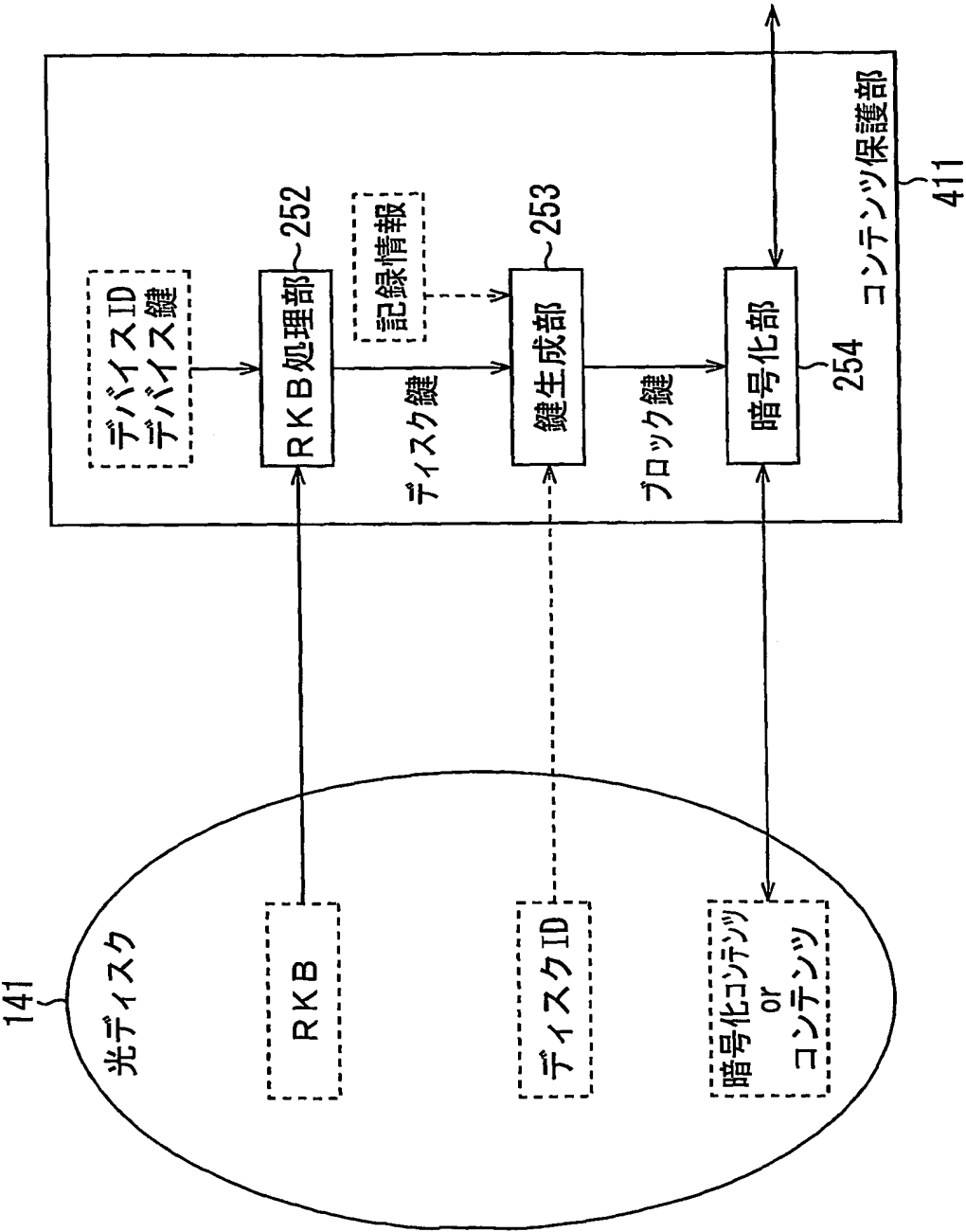


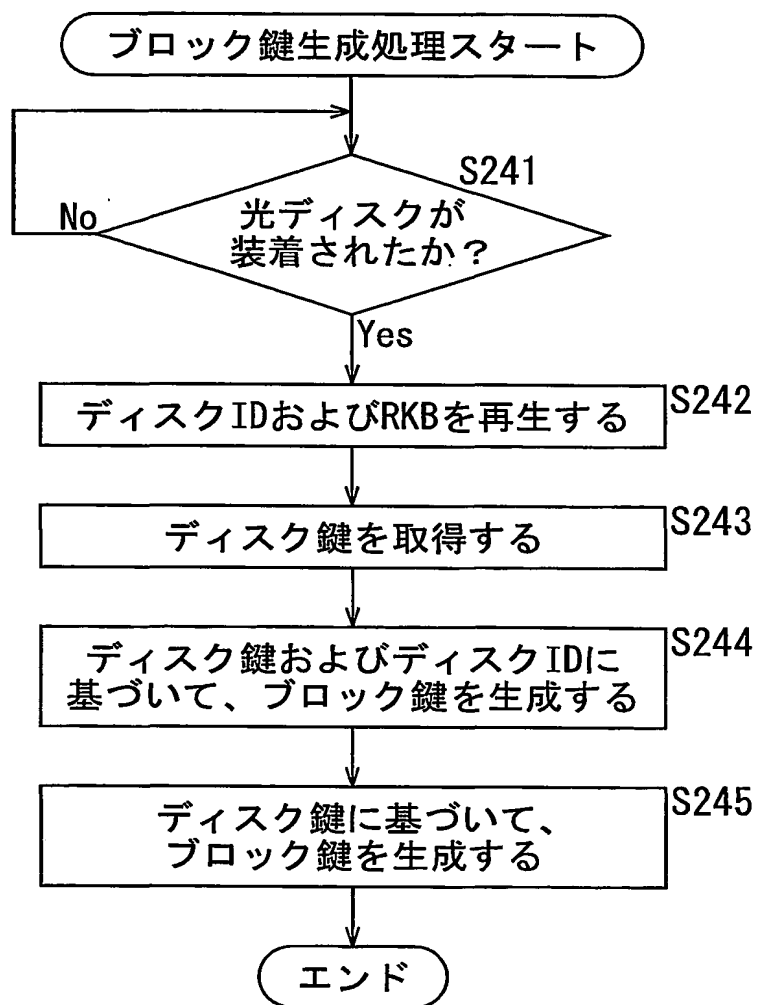
図25





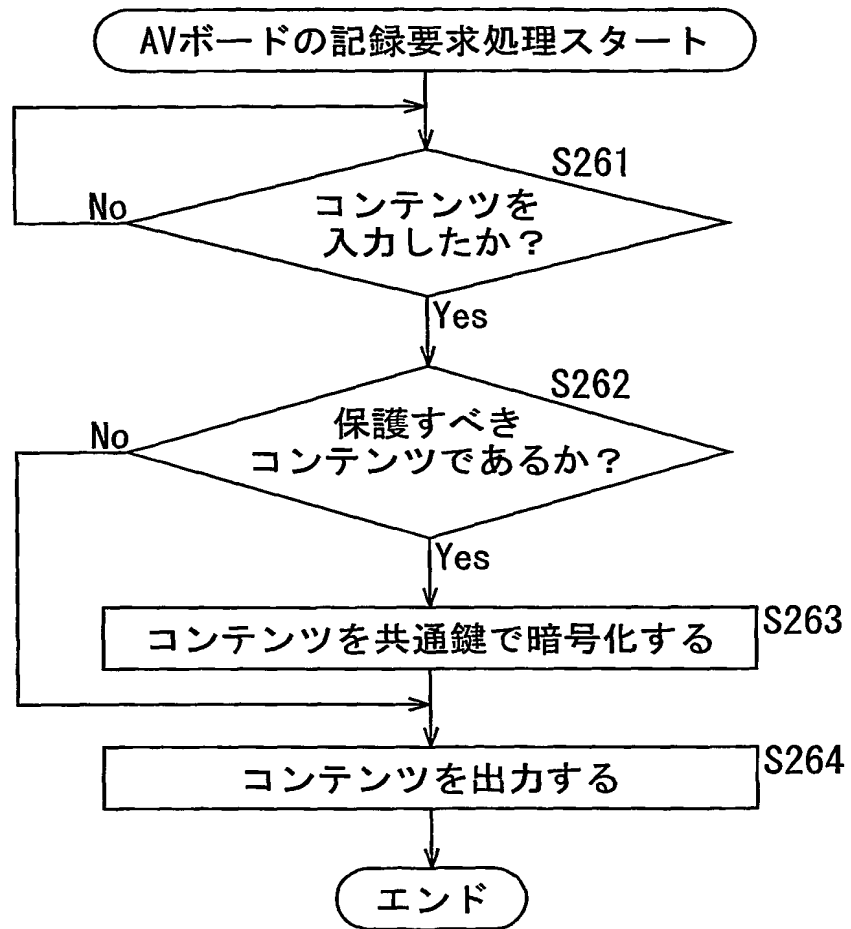
25/33

図26



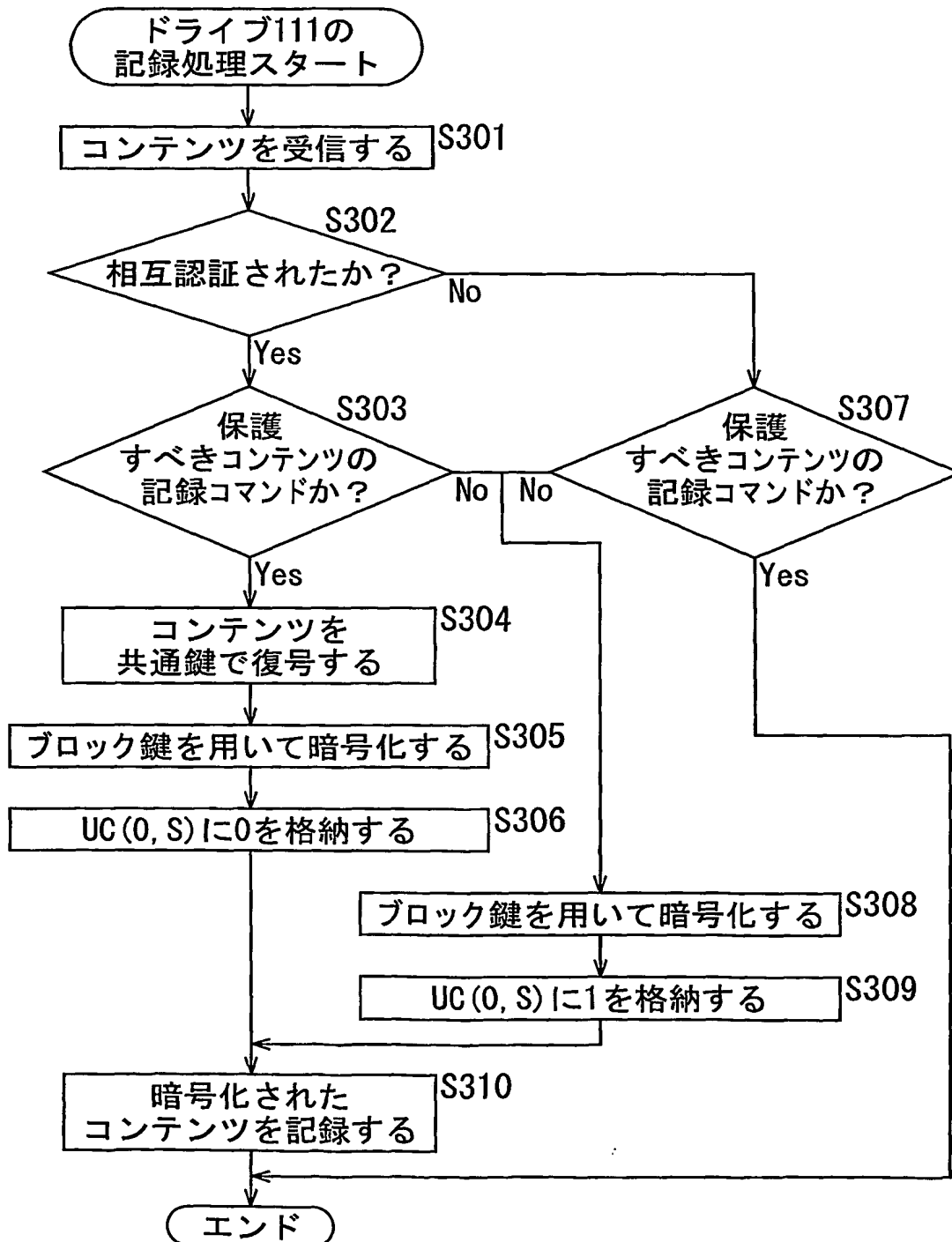
26/33

図27



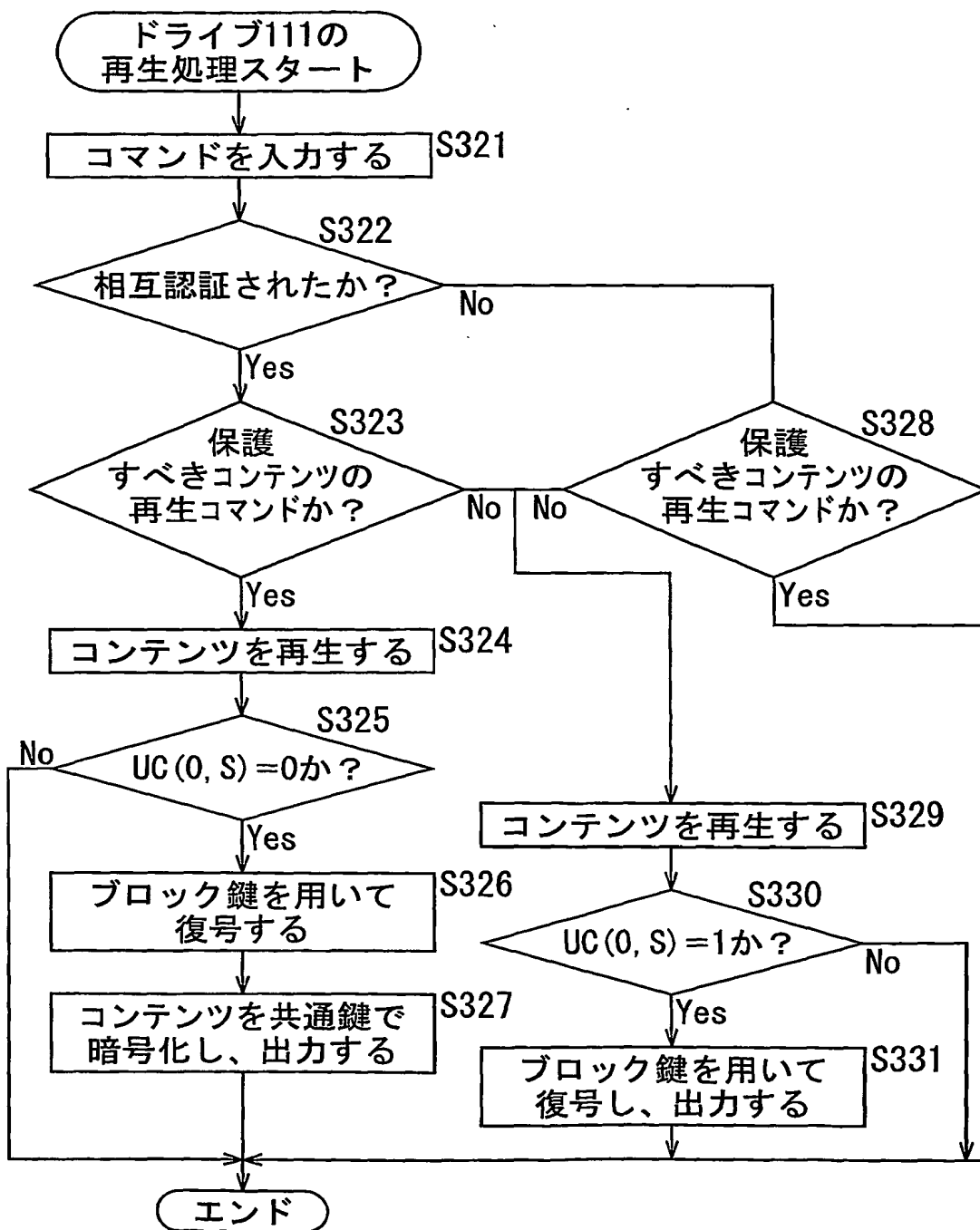
27/33

図28



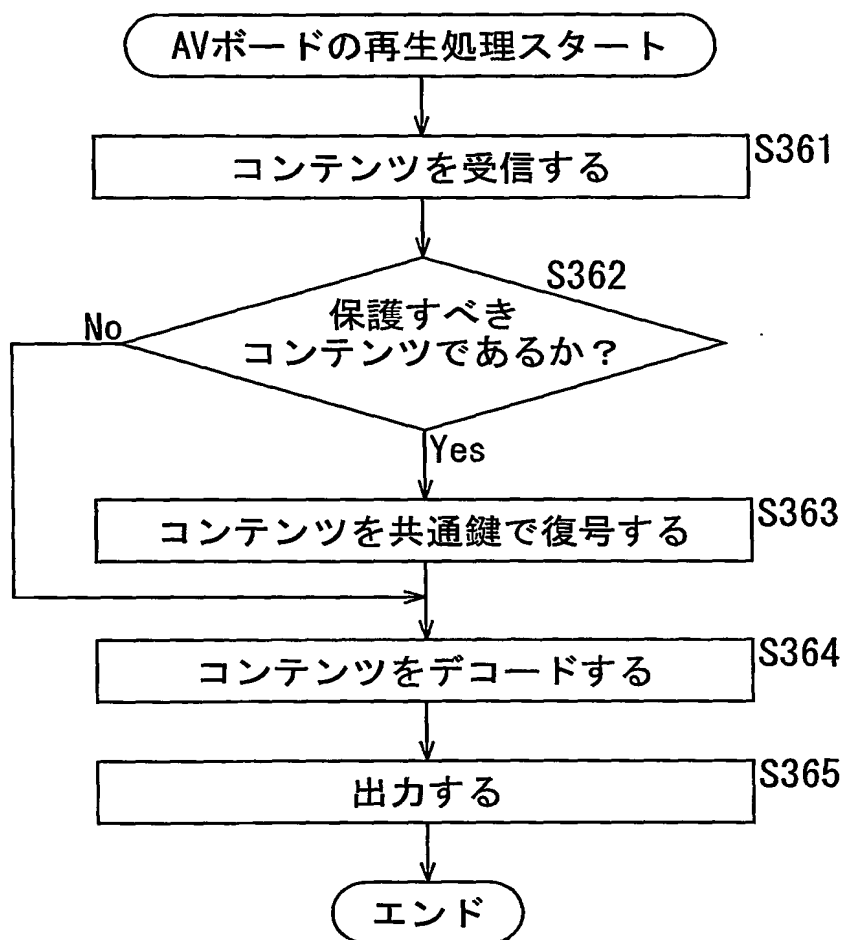
28/33

図29



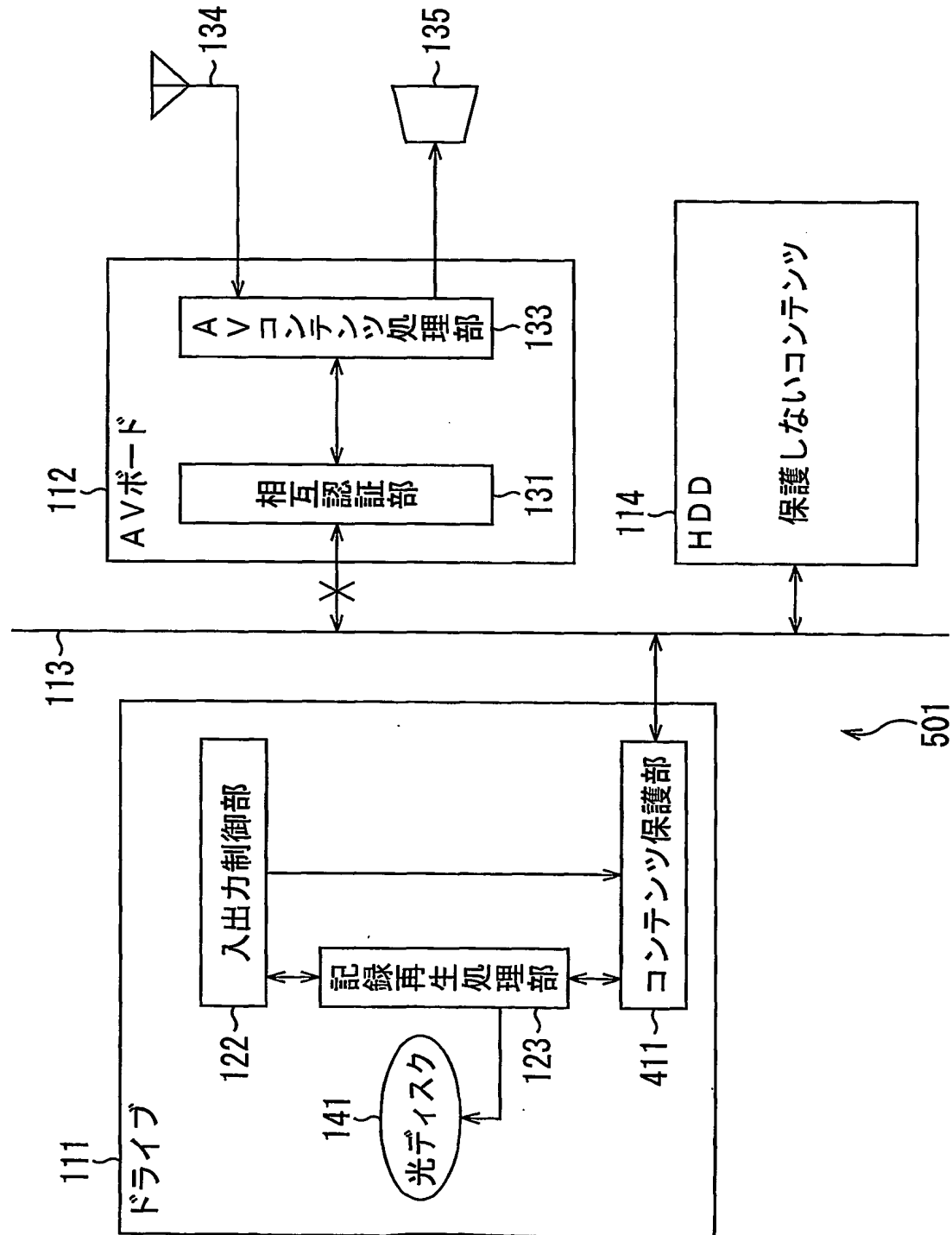
29/33

図30



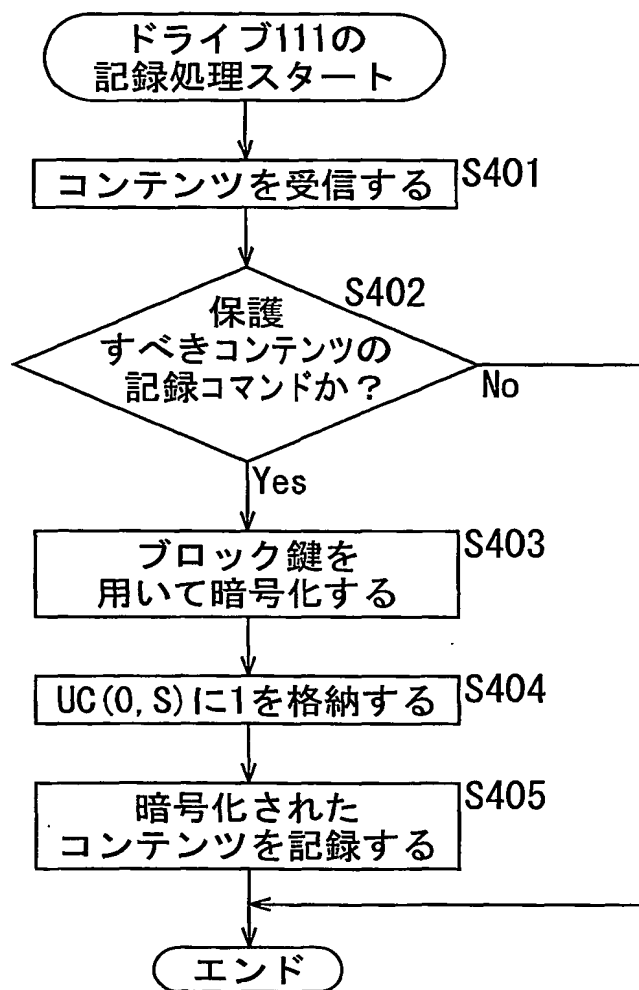
30/33

図31



31/33

図32



32/33

図33

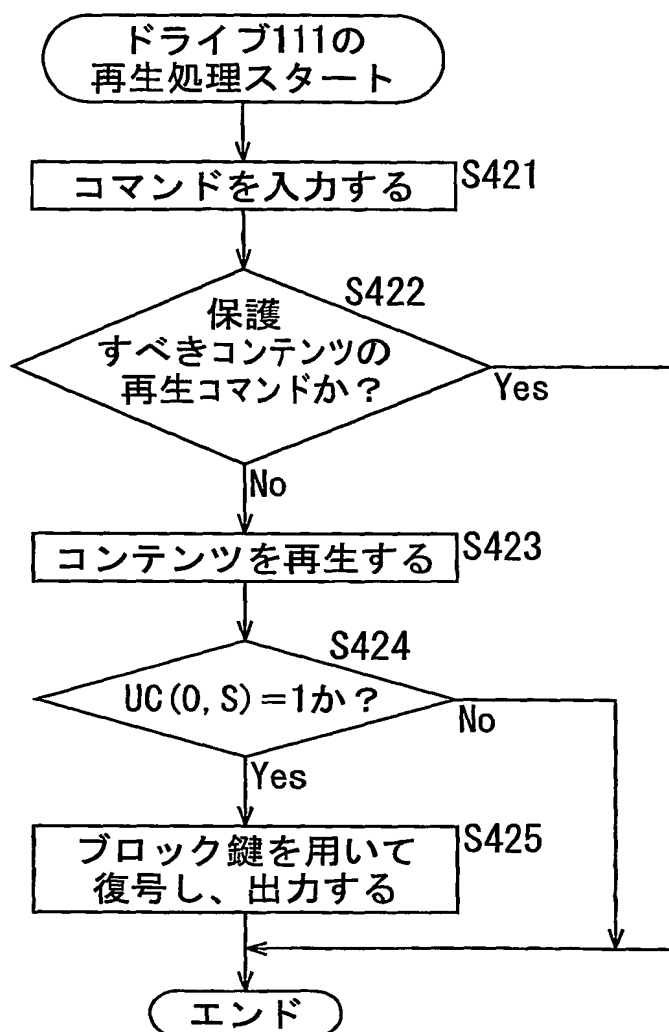
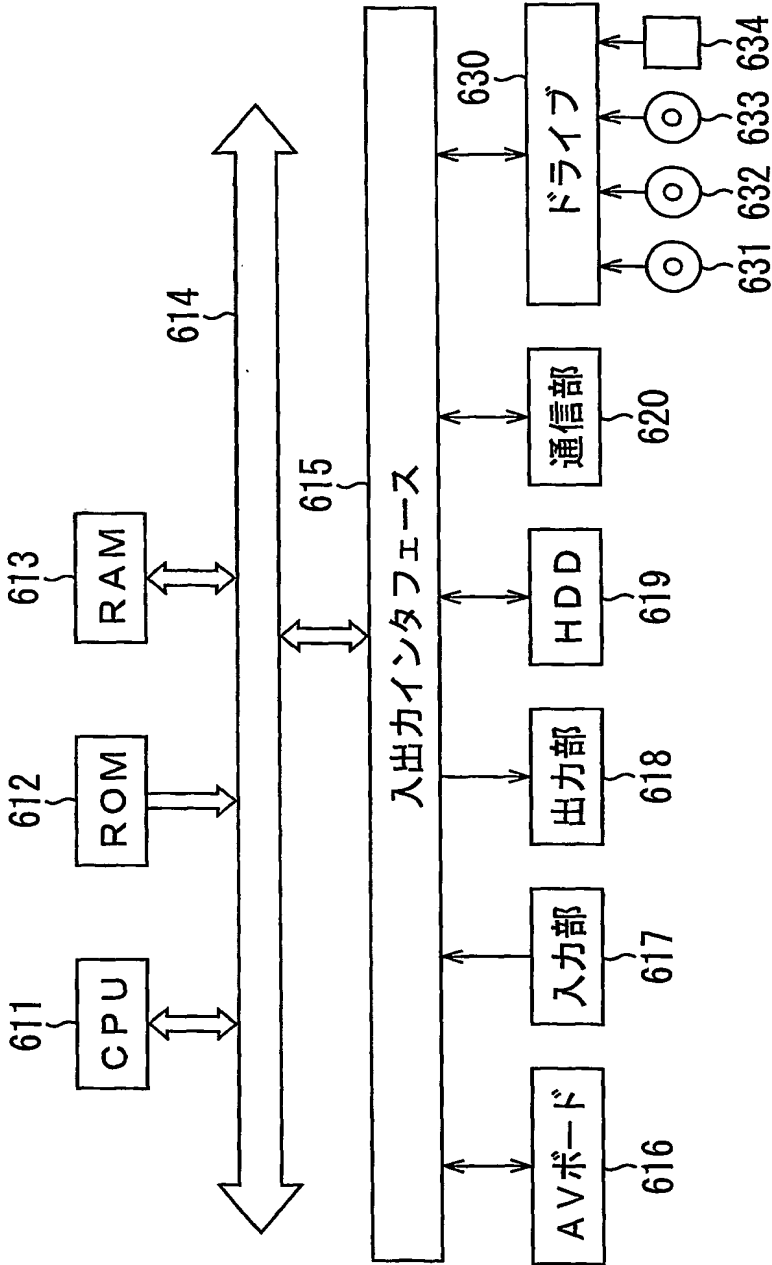




図34



601

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/13752

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F12/14, G09C1/00, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14, G09C1/00, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-285027 A (Matsushita Electric Industrial Co., Ltd.), 13 October, 2000 (13.10.00), All pages; all drawings; particularly, Claim 8 & WO 00/26910 A1 & EP 1045389 A1	1-3, 8, 9, 23-26, 31-34, 37-39 4-7, 10-22, 27-30, 35, 36
Y	JP 2002-84271 A (Sony Corp.), 22 March, 2002 (22.03.02.), All pages; all drawings & EP 1187391 A2	4, 5, 7, 11, 12, 18, 19, 29
Y	"5C Digital Transmission Content Protection White Paper", [online], 14 July, 1998 (14.07.98), DTLA, [retrieved on 08 January, 2004 (08.01.04)], Retrieved from the Internet: <URL: http://www.dtcp.com/data/wp_spec.pdf>	6, 10-22, 27-30, 35, 36

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier document but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
08 January, 2004 (08.01.04)

Date of mailing of the international search report  
27 January, 2004 (27.01.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/13752

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-132457 A (Victor Company Of Japan, Ltd.), 10 May, 2002 (10.05.02), All pages; all drawings; particularly, Par. No. [0068] (Family: none)	1-39
A	JP 2000-187935 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2000 (04.07.00), All pages; all drawings; particularly, Par. No. [0019] & WO 00/05716 A1 & EP 1018733 A1	1-39
A	JP 11-306677 A (Sony Corp.), 05 November, 1999 (05.11.99), All pages; all drawings & EP 938091 A2	1-39

A. 発明の属する分野の分類 (国際特許分類 (IPC)).  
Int. Cl.<sup>7</sup> G06F12/14, G09C1/00, G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))  
Int. Cl.<sup>7</sup> G06F12/14, G09C1/00, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922 - 1996 年  
日本国公開実用新案公報 1971 - 2004 年  
日本国登録実用新案公報 1994 - 2004 年  
日本国実用新案登録公報 1996 - 2004 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-285027 A (松下電器産業株式会社) 2000.10.13, 全頁, 全図, 特に【請求項8】 & WO 00/26910 A1 & EP 1045389 A1	1-3, 8, 9, 23-26, 31-34, 37-39
Y		4-7, 10-22, 27-30, 35, 36
Y	JP 2002-84271 A (ソニー株式会社) 2002.03.22, 全頁, 全図 & EP 1187391 A2	4, 5, 7, 11, 12, 18, 19, 29

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

08.01.2004

国際調査報告の発送日

27.1.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JPO)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

奥村 元宏

5N

3044

電話番号 03-3581-1101

内線 3585

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	"5C Digital Transmission Content Protection White Paper", [online], 1998.07.14, DTLA, [retrieved on 2004-01-08], Retrieved from the Internet: <URL: http://www.dtcp.com/data/ wp_spec.pdf>	6, 10-22, 27-30, 35, 36
A	JP 2002-132457 A (日本ビクター株式会社) 2002.05.10, 全頁, 全図, 特に【0068】段落 (ファミリーなし)	1-39
A	JP 2000-187935 A (松下電器産業株式会社) 2000.07.04, 全頁, 全図, 特に【0019】段落 & WO 00/05716 A1 & EP 1018733 A1	1-39
A	JP 11-306677 A (ソニー株式会社) 1999.11.05, 全頁, 全図 & EP 938091 A2	1-39